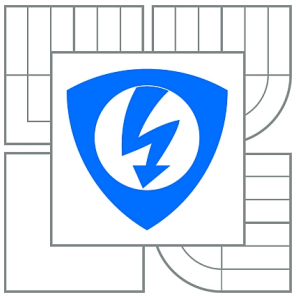
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

BEZPEČNOSTNÍ RIZIKA PŘEPÍNAČŮ

SWITCHES SECURITY RISKS

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

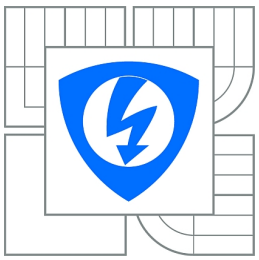
AUTOR PRÁCE — PETER HALAŠKA

AUTHOR

VEDOUCÍ PRÁCE — Ing. JIŘÍ SOBEK

SUPERVISOR

BRNO 2014



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student: Peter Halaška ***ID:*** 146825
Ročník: 3 ***Akademický rok:*** 2013/2014

NÁZEV TÉMATU:

Bezpečnostní rizika přepínačů

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte a následně zpracujte problematiku zabezpečení přepínačů pracujících na druhé vrstvě OSI/ISO modelu. Zmapujte jednotlivé útoky na přepínače a proveďte jejich zhodnocení. Na základě těchto poznatků proveďte vybrané útoky na přepínače a výsledky vhodně prezentujte.

DOPORUČENÁ LITERATURA:

[1] NORTHCUTT, S., ZELTSER, L. Bezpečnost počítačových sítí. Computer Press, 2006. ISBN 80-251-0697-7.
DOSTÁLEK, L. Velký průvodce protokoly TCP/IP: Bezpečnost. 1.vyd. Praha: Computer Press, 2001, 565 s. ISBN 80-722-6513-X.
[2] HUCABY, D. CCNP SWITCH 642-813 official certification guide. Indianapolis: Cisco Press, c2010, xxvii, 459 s. ISBN 978-1-58720-243-8.

Termín zadání: 10.2.2014 ***Termín odevzdání:*** 4.6.2014

Vedoucí práce: Ing. Jiří Sobek
Konzultanti bakalářské práce:

doc. Ing. Jiří Mišurec, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Cieľom tejto bakalárskej práce bolo preštudovať a následne spracovať problematiku zabezpečenia prepínačov pracujúcich na spojovej vrstve OSI/ISO modelu. Zmapovať jednotlivé útoky na prepínače spolu s ich zhodnotením. Na základe týchto poznatkov vykonať vybrané útoky na prepínače a výsledky vhodne prezentovať.

KĽÚČOVÉ SLOVÁ

prepínač, bezpečnosť, útok, spojová vrstva

ABSTRACT

The aim of this thesis was to study and subsequently process issues of securing switches operating at the data link layer of OSI/ISO model. Map individual switch attacks with their review. On the basis of this information realize chosen attacks with presented results.

KEYWORDS

switch, security, attack, data link layer

HALAŠKA, Peter. *Bezpečnostní rizika přepínačů*: bakalárska práca. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2014. 98 s. Vedúci práce bol Ing. Jiří Sobek.

PREHLÁSENIE

Prehlasujem, že som svoju bakalársku prácu na tému „Bezpečnostní rizika přepínačů“ vypracoval samostatne pod vedením vedúceho bakalárskej práce, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej bakalárskej práce ďalej prehlasujem, že v súvislosti s vytvorením tejto bakalárskej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka č. 40/2009 Sb.

Brno ....

(podpis autora)

POĎAKOVANIE

Rád by som poďakoval vedúcemu bakalárskej práce, pánovi Ing. Jiřímu Sobkovi, za odborné vedenie, konzultácie, trpezlivosť a podnetné návrhy k práci.

Brno ....

(podpis autora)

OBSAH

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ÚVOD

Lokálne siete (LAN) sú v súčasnej dobe neoddeliteľnou súčasťou budov rôznych inštitúcií ako sú firmy, školy apod. Ich zabezpečenie je často neprávom obchádzané a pritom veľká časť všetkých útokov je vykonávaná práve v lokálnych sieťach. [1]

Ethernetové prepínače sú v súčasnej dobe ľahko inštalovateľné a nastaviteľné, tým pádom je veľmi jednoduché zabudnúť na ich bezpečnosť napriek tomu, že v spojitosti s nimi existuje mnoho zraniteľných miest. Programy pre ich zneužitie (napr. *Dsniff*) sa začali objavovať už pred niekoľkými rokmi. S týmito ľahko použiteľnými programami môže útočník jednoducho odkloniť tok dát cez jeho zariadenie s ich následným zneužitím alebo zahltiť atakované zariadenie nevyžiadaným dátovým tokom za účelom vyčerpania jeho výpočtového výkonu. [2]

Cieľom tejto bakalárskej práce je zmapovať najčastejšie útoky na prepínače, prakticky ich vykonať a na základe získaných poznatkov vykonať ich zhodnotenie.

V prvej časti teoretického úvodu sa práca venuje predovšetkým technológiam Ethernet a ich základným pojmom súvisiacim s komunikáciu v lokálnych sieťach, ako je *CSMA/CD*, *Half-Duplex*, *Full-Duplex* atď. Keďže sa v práci jedná predovšetkým o prepínače pracujúce na spojovej vrstve, je v tejto časti popísaný aj ethernetový rámec s jeho základnými časťami.

Druhá časť práce sa venuje samotnému popisu ethernetového prepínača a objasňuje jeho základnú funkciu a činnosť v LAN sieťach, a to predovšetkým procesu učenia MAC adries a význam CAM tabuľky v jeho rozhodnutiach.
Ďalej sú v tejto časti vysvetlené pojmy ako *unicast*, *multicast* a *broadcast*.

Tretia, najobsiahlejšia časť teoretického úvodu, mapuje najčastejšie, v praxi vykonávané útoky na prepínače. V práci je uvedených dokopy šesť útokov a každý je definovaný v troch častiach: **charakteristika** útoku, **detekcia** útoku a **ochrana** voči útoku. Dodatočne sú pri každom útoku objasnené niektoré pojmy pre jeho lepšie pochopenie.

Nasledujúca teoretická časť sa venuje popisu programového vybavenia, pomocou ktorého boli vybrané útoky uskutočňované.

Útoky boli vykonávané na prepínače od firmy Hewlett-Packard a Cisco, ktoré patria medzi najpoužívanejšie v prostredí inštitúcií. Posledná teoretická časť práce je venovaná ich stručnému popisu.

Praktická časť bakalárskej práce sa venuje samotnému vykonaniu vybraných útokov. Každý vykonaný útok je popísaný v troch častiach: **vykonanie** útoku, **aplikácia ochrany** voči útoku a **vyhodnotenie** útoku.

Záverečná časť práce sa venuje celkovému vyhodnoteniu, ktoré vzniklo na základe získaných teoretických a praktických poznatkov.

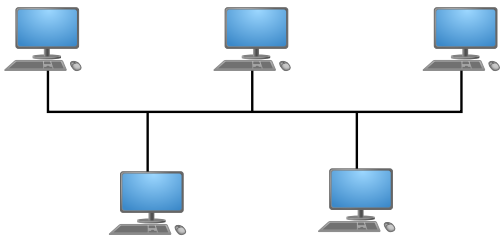
1 TECHNOLÓGIE ETHERNET

Ethernet predstavuje súbor technológií pre lokálne siete pokrytých štandardom IEEE 802.3 a umožňuje všetkým zariadeniam v sieti využívať zdieľané médium a jeho šírku pásma. Prvá experimentálna verzia technológií Ethernet bola vyvinutá v roku 1973 v laboratóriach firmy Xerox pracujúca na prenosovej rýchlosti 2,94 Mbit/s. V roku 1980 bola štandardizovaná a predstavená jej prvá verzia pre komerčné využitie pracujúca na prenosovej rýchlosti 10 Mbit/s. S príchodom nových verzií a technológií sa jej prenosová rýchlosť časom zvyšovala.
V aktuálnej dobe sa využívajú prenosové rýchlosti:

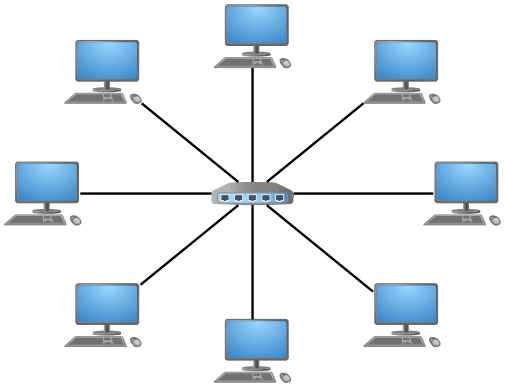
- 10 Mbit/s – Ethernet,
- 100 Mbit/s – Fast Ethernet,
- 1 Gbit/s – Gigabitový Ethernet,
- 10 Gbit/s – 10gigabitový Ethernet.

Ako prenosové média boli v minulosti využívané koaxiálne káble, no v dnešnej dobe sú v popredí predovšetkým krútené dvojlinky a optické káble. Ethernetová sieť využíva pre prístup zariadenia na zdieľané médium algoritmus CSMA/CD (Carrier Sense Multiple Access with Collision Detection). V ethernetovej sieti sa uplatňujú aktívne sieťové zariadenia ako rozbočovač, most, prepínač a okrajovo aj smerovač. Z hľadiska zapojenia koncových zariadení Ethernet podporuje v minulosti využívanú zbernicovú (anglicky Bus) a dnes preferovanú hviezdicovú (anglicky Star) topológiu.

Vďaka jednoduchosti inštalácie, udržovateľnosti, nízkej cene a flexibilite si oproti ostatným technológiam (Token Ring, FDDI, . . .) udržala rolu majoritnej technológie v oblasti LAN sietí. [17, 14]



Obr. 1.1: Zbernicová topológia.



Obr. 1.2: Hviezdicová topológia.

1.1 CSMA/CD

Carrier Sense Multiple Access with Collision Detection

Ethernet bol pôvodne navrhnutý pre využívanie zdieľaného média. To umožnilo dvom alebo viacerým koncovým zariadeniam využívať rovnaké fyzické médium, a tak medzi sebou komunikovať. Protokol CSMA/CD bol vytvorený za účelom riešenia kolízií, ktoré nastanú, keď dve (respektíve viaceré) zariadenia vysielajú dáta v rovnakom čase.
Rozlišujeme dve metódy komunikácie na zdieľanom fyzickom médiu:

- **Half-Duplex** – polovičný duplex,
- **Full-Duplex** – plný duplex.

1.1.1 Half-Duplex

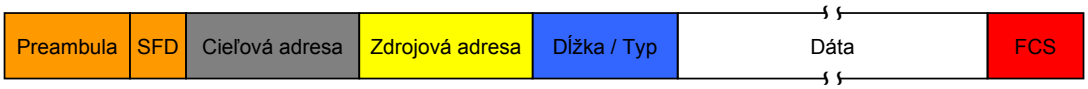
Komunikácia využívajúca ako prenosové médium koaxálny kábel nemumožňovala v základnom frekvenčnom pásme využívať súčasne vysielanie aj príjem dát. Preto je nutné využívať poloduplexnú komunikáciu. Pri použití krútenej dvojlinky je na príjem aj odosielanie určený jeden pár vodičov pre oba smery.
Protokol CSMA/CD sa uplatňuje v polovičnom duplexe za účelom kontrolovania prístupu na médium. *Carrier sense* špecifikuje, že zariadenie načúva danému fyzickému médiu, aby zistil, či ním nie je prenášaný signál od iného zariadenia. Pokiaľ je médium voľné a tzv. interframe gap interval je vyčerpaný, stanica zaháji prenos. Interframe gap je minimálny časový interval medzi posielanými rámcami. Pre klasický Ethernet predstavuje 9,6 µs, pre Fast Ethernet 0,96 µs atď.
Pokiaľ v jednom okamžiku vysielajú dáta dve (respektíve viaceré) zariadenia súčasne, nastáva kolízia. To činí kolidované rámce nerozlúštiteľnými. Akonáhle je na danom segmente zistená kolízia, obidve stanice ukončia vysielanie a vyšlú tzv. jam signál, aby na kolíziu upozornili ostatné stanice v segmente. Ďalej stanice inkrementujú číselnú hodnotu v počítadle pokusov, ktorých maximálny počet je 15, pričom šestnásty pokus znamená zahodenie rámca. Následne budú obidve zariadenia čakať náhodne vygenerovaný časový interval, aby znížili pravdepodobnosť ďalšej kolízie. Po tomto čase opäť začnú preposielať rámce. O tento proces sa stará tzv. backoff algoritmus.
Typickým LAN zariadením, ktoré sa využíva v polovične duplexnej komunikácii je rozbočovač, ktorý rámec ihneď po obdržaní všesmerovo preposiela všetkými jeho rozhraniami okrem toho, ktorým rámec prijal, a sám tvorí jednu kolíznu doménu. [8, 5, 14]

1.1.2 Full-Duplex

Na rozdiel od polovičného duplexu, plný duplex podporuje súčasne odosielanie aj prijímanie dát, a to za pomoci dvoch párov vodičov krútenej dvojlinky, pričom jeden slúži na odosielanie a druhý na príjímanie dát. Pri použití optického káblu môžeme pre plne duplexnú komunikáciu využívať buď jedno vlákno pre prijímanie a druhé pre odosielanie, alebo použijeme optické signály s rôznou vlnovou dĺžkou. Na základe tohto oddelenia sa efektívne zdvojnásobila priechodnosť sieťového rozhrania zariadenia. Aby mohla nastať plne duplexná komunikácia, musí byť medzi odosielateľom a prijímateľom dát vytvorené spojenie typu *bod-bod* (anglicky *point-to-point*). A pretože sú dáta odosielané na oddelených pároch vodičov, žiadna kolízia nenastane. Tým pádom sa v plnom duplexe naďalej nevýužíva protokol CSMA/CD.
Typickým LAN zariadením, ktoré sa využíva v plne duplexnej komunikácii je prepínač, kde každé jeho sieťové rozhranie vytvára jednu kolíznu doménu. [8, 5, 14]

1.2 Ethernetový rámec

Spojová vrstva je zodpovedná za zlučovoanie bitov do bajtov a bajtov do ethernetových rámcov. Tieto rámce sú využívané spojovou vrstvou na zapúzdrenie paketov obdržaných od vyššej (sieťovej) vrstvy OSI modelu za účelom odovzdania dátovej jednotky fyzickej vrstve a následného odoslania na prenosové médium.



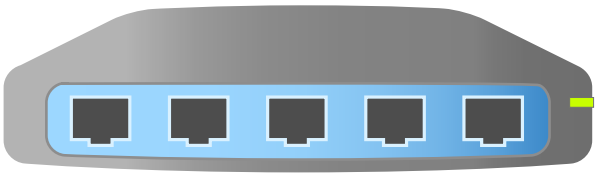
Obr. 1.3: Základná štruktúra ethernetového rámca.

- **Preambula** – pozostáva zo siedmich bajtov a jej štruktúru tvoria striedajúce sa logické `0` a `1`. Slúži na synchronizáciu hodín príjemcu rámca,
- **SFD** (Start Frame Delimiter) – pozostáva z jedného bajtu a slúži na označenie začiatku rámca. Hodnota SFD je `10101011`, kde posledné `11` umožňujú príjemcovi rozpoznať začiatok rámca a zosynchronizovať sa, aj keby nezaznamenal začiatok preambuly,
- **Cieľová adresa** – MAC adresa cieľového sieťového rozhrania o dĺžke 48 bitov,
- **Zdrojová adresa** – MAC adresa zdrojového sieťového rozhrania,
- **Dĺžka / Typ** – skladá sa z dvoch bajtov a poskytuje rozdielné funkcie v závislosti na štandarde. Ethernet II používa Typ na identifikáciu použitého sieťového protokolu a 802.3 využíva Dĺžku, ktorá poskytuje údaj o veľkosti rámca,

- **Dáta** – jedná sa o paket, ktorý bol obdržaný od vyššej vrstvy. Jeho veľkosť môže byť 64 až 1500 bajtov,
- **FCS** (Frame Check Sum) – pole, ktoré slúži na detekciu chýb vzniknutých pri prenose. Obsahuje 32bitovú CRC (Cyclic Redundancy Check) hodnotu, ktorá je vytvorená odosielateľom rámca. Počíta sa na základe obsahu rámca od cieľovej adresy až po koniec dátového poľa. Následne je prijímateľom rámca prepočítaná a skontrolovaná zhoda s odosielateľom. [5, 14]

2 PREPÍNAČ

Prepínač (anglicky switch) je aktívne zariadenie počítačovej siete a jeho hlavnou úlohou je prepájať sieťové segmenty a tým zabezpečiť konektivitu medzi zariadeniami v lokálnej sieti. Najrozšírenejším typom je ethernetový prepínač. Z hľadiska spracovania dátových jednotiek sa môžeme v praxi stretnúť predovšetkým s prepínačom pracujúcim na spojovej vrstve (ďalej ako „prepínač“). V oblasti počítačových sietí figuruje ako nástupca rozbočovača (anglicky hub).



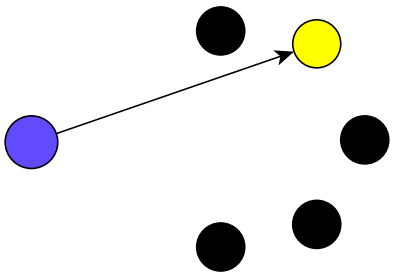
Obr. 2.1: Schematická značka prepínača.

2.1 Funkcia prepínača

Ako už bolo v práci uvedené, prepínač pracuje na spojovej vrstve OSI modelu. To znamená, že jeho dátová jednotka – PDU (Protocol Data Unit) je ethernetový rámec. V ňom sa nachádzajú nevyhnutné informácie, ktoré využíva k jeho základnej činnosti a to predovšetkým MAC (Media Access Control) adresy. MAC adresa je jedinečné identifikačné 48bitové číslo v hexadecimálnom tvare, ktoré slúži na presnú identifikáciu sieťového rozhrania v LAN sieti. Jedinečnosť prvých troch bajtov zaručuje organizácia IEEE (Institute of Electrical and Electronics Engineers), táto časť adresy sa nazýva unikátna identifikácia organizácie (anglicky Organizationally Unique Identifier, OUI) a jedinečnosť posledných troch bajtov zaručuje samotný výrobca sieťového adaptéra. MAC adresa je obsiahnutá v ethernetovom rámci, a to ako v podobe zdrojovej, tak aj cieľovej. Na základe cieľovej MAC adresy môžeme komunikáciu v LAN sieťach rozdeliť na *unicast*, *multicast* a *broadcast*. [5, 8]

Unicast

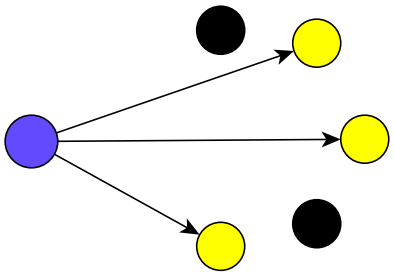
Individuálna komunikácia – predstavuje zasielanie dát od jedného užívateľa k druhému konkrétnemu užívateľovi.
Individuálna adresa môže mať podobu napríklad `04:7d:7b:da:9c:c7`.



Obr. 2.2: Grafické znázornenie komunikácie na báze unicast.

Multicast

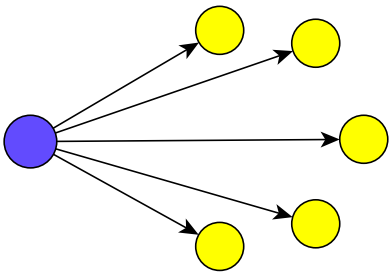
Skupinová komunikácia – umožňuje komunikáciu jedného užívateľa s určitou skupinou užívateľov.
Skupinové adresy sa nachádzajú v rozsahu `01:00:5e:00:00:00` – `01:00:5e:7f:ff:ff`.



Obr. 2.3: Grafické znázornenie komunikácie na báze multicast.

Broadcast

Všesmerová komunikácia – nastáva, keď jedno zariadenie posiela dáta všetkým zariadeniam v danej všesmerovej doméne, čiže všetkým zariadeniam vo vyhradenom adresnom priestore.
Všesmerová adresa má tvar `ff:ff:ff:ff:ff:ff`. [5, 14]



Obr. 2.4: Grafické znázornenie komunikácie na báze broadcast.

Prepínač pre svoju funkciu v LAN sieti musí vykonávať tri hlavné funkcie:

- Učiť sa MAC adresy na základe skúmania zdrojových adries každého rámca prijatého od vysielacieho zariadenia,
- rozhodovať sa, kedy preposlať a kedy odfiltrovať rámec na základe cieľovej MAC adresy,
- vytvárať bezslučkové prostredie v prípade zapojenia viacerých prepínačov v LAN sieti.

Rozhodovanie, kam preposlať rámec spočíva v tom, že prepínač používa dynamicky vytvorenú databázu, ktorá obsahuje zoznam MAC adries zariadení pripojených do daného prepínača spolu s odchádzajúcimi rozhraniami, ktoré k ním vedú. Táto databáza sa nazýva CAM (Content-Addressable Memory) tabuľka. Prepínač porovnáva cieľové MAC adresy umiestnené v prijatom ethernetovom rámci spolu s adresami v jeho CAM tabuľke a na základe toho uskutoční rozohodnutie, kam daný rámec preposlať, respektíve ho ignoruje.

Prepínač má však po jeho zapnutí CAM tabuľku prázdnu, tým pádom sa potrebné MAC adresy musí naučiť, aby mohol uskutočňovať správne rozhodnutia. Svoju CAM tabuľku si vybuduje načúvaním prichádzajúcich rámcov a skúmaním zdrojových MAC adries nachádzajúcich sa v nich. Pokiaľ sa zistená zdrojová MAC adresa nenachádza v jeho CAM tabuľke, prepínač ju do nej umiestni spolu s rozhraním, cez ktoré rámec obdržal. Avšak nastáva otázka, kam preposlať rámec, ktorého cieľová adresa sa nenachádza v CAM tabuľke? V tomto prípade prepínač všesmerovo preposiela daný rámec všetkými jeho rozhraniami okrem toho, ktorým rámec obdržal s tým, že očakáva odpoveď od cieľovej stanice, pre ktorú bol rámec určený. Pokiaľ stanica na tento rámec odpovie, prepínač si umiestni jej adresu spolu s rozhraním, ktoré k nej vedie do svojej CAM tabuľky. [14]

3 NAJČASTEJŠIE ÚTOKY NA PREPÍNAČE

3.1 MAC flooding

3.1.1 Charakteristika útoku

CAM tabuľka prepínača je schopná uchovávať len určité množstvo MAC adries naraz. Ich počet závisí predovšetkým na type prepínača, na ktorý sa daný útok vykonáva. Najlacnejšie prepínače podporujú malé počty MAC adries, no najvýkonnejšie zariadenia sú schopné uchovávať viac než 100 000 záznamov. Prepínač na základe časovaču životnosti MAC adries monitoruje záznamy v CAM tabuľke a vynuluje sa v situácii, keď prepínač obdrží rámec so zdrojovou MAC adresou rovnakou, aká sa už nachádza v jeho CAM tabuľke. Pokiaľ prepínač neobdrží takýto rámec pred tým, než časovač životnosti vyprší, vymaže daný záznam z jeho CAM tabuľky. Tento časovač sa nazýva *aging timer*.
Útočník narúša funkciu prepínača tým, že vysiela prúd rámcov s náhodne vygenerovanými zdrojovými a cieľovými MAC adresami. Napriek tomu, že útočník vykonáva útok z jedného zariadenia, rámce javia ako prichádzajúce z niekoľkých staníc. Tieto stanice sú však fiktívne a irelevantné, hlavným cieľom je jednoducho zaplniť CAM tabuľku prepínača. Akonáhle je táto tabuľka zaplnená, prepínač začne preposielať prijaté rámce všesmerovo každým rozhraním okrem toho, ktorým rámce prijal. Útočník využije túto situáciu vo svoj prospech a tým má umožnené odchytávanie citlivých dát, ktoré vysielajú stanice pripojené k danému prepínaču za podmienky, že má svoju sieťovú kartu nastavenú v promiskuitnom režime.
Vzhľadom na to, že prepínač, na ktorom je vykonávaný útok preposiela rámce všesmerovo, sú ovplyvnené aj ostatné prepínače vo všesmerovej doméne. Táto situácia môže viesť k domino efektu pre koncové zariadenia, a tak môžeme pozorovať situáciu, kde nastáva odoprenie služby (anglicky Denial of Service, DoS). [2, 10]

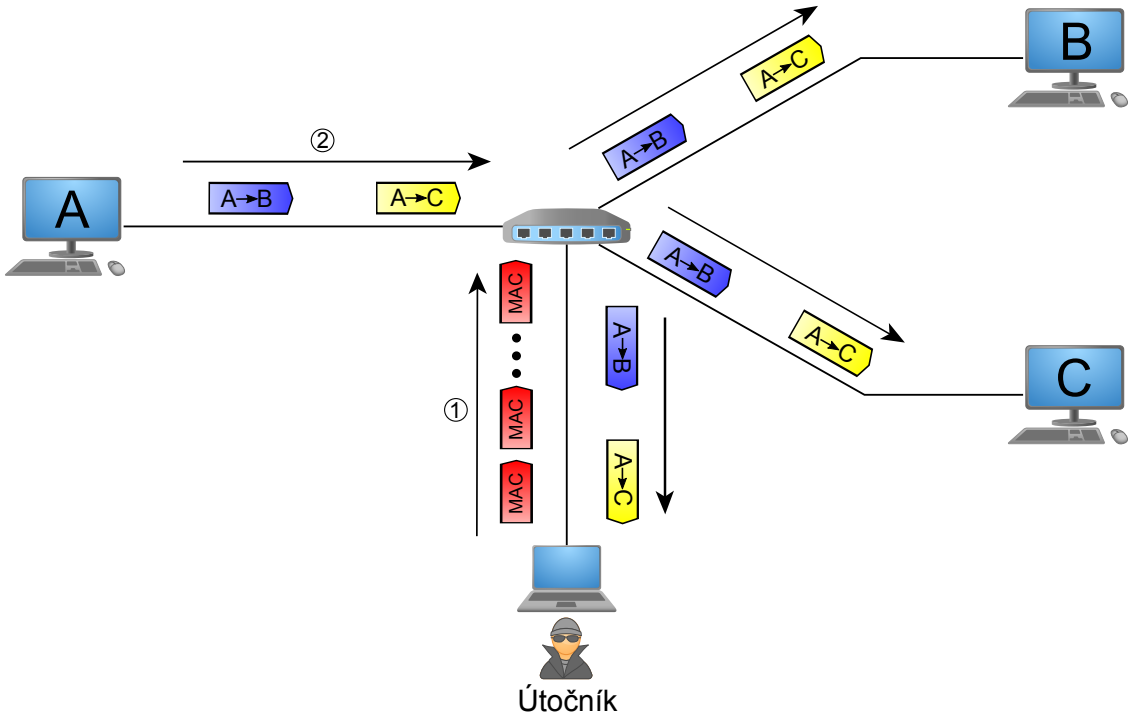
3.1.2 Detekcia útoku

Útok možno najlepšie detegovať vypísaním CAM tabuľky na manažovateľných prepínačoch. Ďalším spôsobom detekcie je aj pasívne monitorovanie siete, pokiaľ má administrátor svoju sieťovú kartu nastavenú v promiskuitnom režime. Musí však byť pripojený na rovnaký prepínač ako útočník. Pokiaľ administrátor zaznamená príjem rámcov, ktoré su určené iným cieľovým MAC adresám, ako je jeho, s vysokou pravdepodobnosťou sa jedná o MAC flooding útok.

3.1.3 Ochrana voči útoku

Zabezpečenie rozhrania (port security)

Jednou z často používaných možností k ochrane voči tomuto typu útoku je manuálne nakonfigurovanie MAC adresy k danému rozhraniu. Táto možnosť síce môže byť efektívna, no nie vždy optimálna vzhľadom na to, že môžu nastať určité nezhody s niektorými používanými sieťovými aplikáciami. Avšak v prípade niektorých prepínačov, predovšetkým lacnejších, je táto možnosť zabezpečenia rozhrania jediná. Niektoré z týchto zariadení podporujú podobnú funkciu s tým rozdielom, že sa MAC adresu dokážu dynamicky naučiť a následne k nej priradiť dané rozhranie.
Niekoľko výrobcov prepínačov (Cisco, Nortel, . . .) však umožnilo na ich zariadeniach rozšírenú konfiguráciu zabezpečenia rozhraní. Okrem základných funkcií umožňujú nastavenie rôznych parametrov, ako je limitovanie počtu používaných MAC adries, oznámenie o narušení bezpečnosti rozhrania, respektíve vypnutie rozhrania pri nesplnení užívateľom nastavenej bezpečnostnej podmienky. [2, 10, 3]



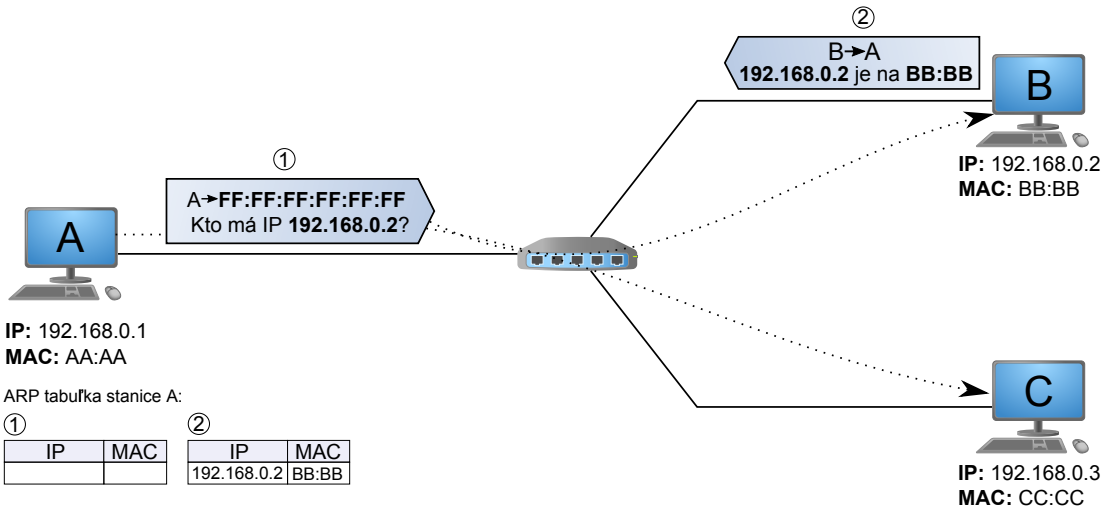
Obr. 3.1: Grafické znázornenie útoku MAC flooding.

3.2 ARP spoofing

ARP (Address Resolution Protocol) je protokol spojovej vrstvy OSI modelu zabezpečujúci mapovanie IP adries na MAC adresy sieťových uzlov. Aby mohol byť rámec obsahujúci paket odoslaný v danej LAN sieti správnemu adresátovi na základe cieľovej IP adresy, musí odosielajúce zariadenie poznať MAC adresu príjemcu. Medzi IP adresou a MAC adresou totiž neexistuje žiadna matematická spojitosť, preto zariadenie pred odoslaním hľadá záznam v jeho ARP tabuľke (anglicky ARP cache).

Proces určenia MAC adresy prebieha tak, že zariadenie vykoná operáciu logického súčinu medzi IP adresou a maskou siete, v ktorej je pripojené, aby zistil, či sa daná cieľová stanica nachádza v jeho lokálnej sieti alebo mimo nej. Pokiaľ zistí, že sa cieľová stanica nachádza v jeho lokálnej sieti, zariadenie hľadá v jeho ARP tabuľke príslušnú MAC adresu. Ak zistí, že sa cieľová stanica nenachádza v jeho lokálnej sieti, tak priradí cieľovú MAC adresu príslušnej bráne (anglicky gateway). V prípade brány sa najčastejšie jedná o smerovač, ktorý vedie do WAN siete, respektíve internetu.

Pokiaľ sa v ARP tabuľke nenachádza príslušná MAC adresa pre IP adresu, zariadenie vyšle ARP požiadavku (anglicky ARP request), ktorou žiadá o MAC adresu k príslušnej IP adrese. Po obdžaní ARP odpovede (anglicky ARP reply) od cieľovej stanice si zariadenie vloží údaj do jeho ARP tabuľky. Tento údaj má životnosť určitú dobu, pokiaľ nedôjde k jeho obnoveniu. Táto doba závisí od používaného operačného systému na danom zariadení. [5, 2]



Obr. 3.2: Grafické znázornenie procesu žiadosti a odpovede v ARP protokole (MAC adresy koncových staníc sú kvôli prehľadnosti v zjednodušenom tvare). [2]

Bezpečnosť ARP

S ohľadom na bezpečnosť, protokol ARP je charakterizovaný tromi hlavnými nevýhodami:

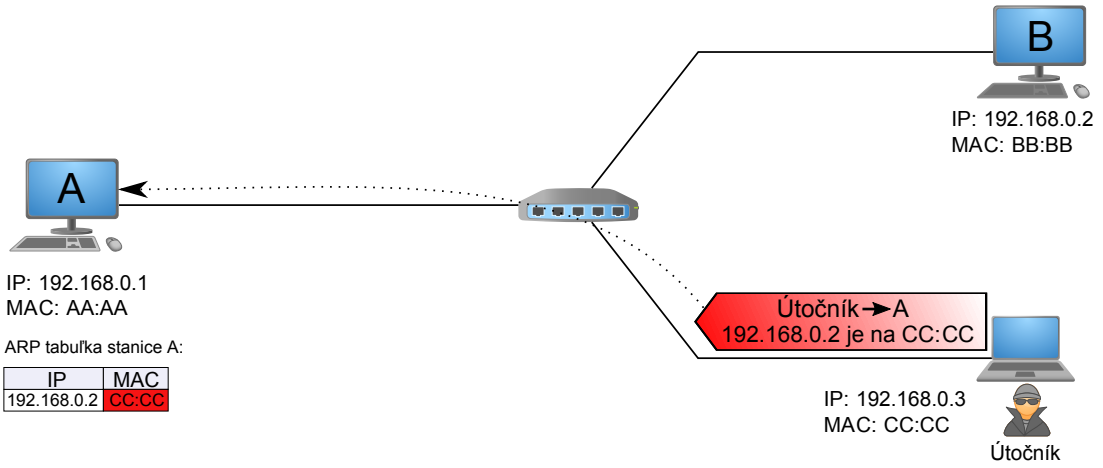
- **Neprítomnosť autentifikácie** – stanica, ktorá odpovedá na ARP žiadosť žiadnym spôsobom neoznačí ARP paket s odpoveďou, tým pádom nie je nijako zaručená integrita dát,
- **únik informácií** – v dôsledku všesmerovo posielanej ARP žiadosti sa všetky koncové stanice v danej lokálnej sieti môžu dozvedieť, že jedna stanica chce komunikovať s druhou,
- **problém dostupnosti** – tým, že všetky stanice v jednej všesmerovej doméne obdržia paket s ARP žiadosťou, musia ho spracovať. Útočník môže poslať tisíce ARP žiadostí za sekundu, ktoré musia byť spracované sieťovými zariadeniami. To vedie k plytvaniu šírky pásma a zaťaženiu CPU. [2]

3.2.1 Charakteristika útoku

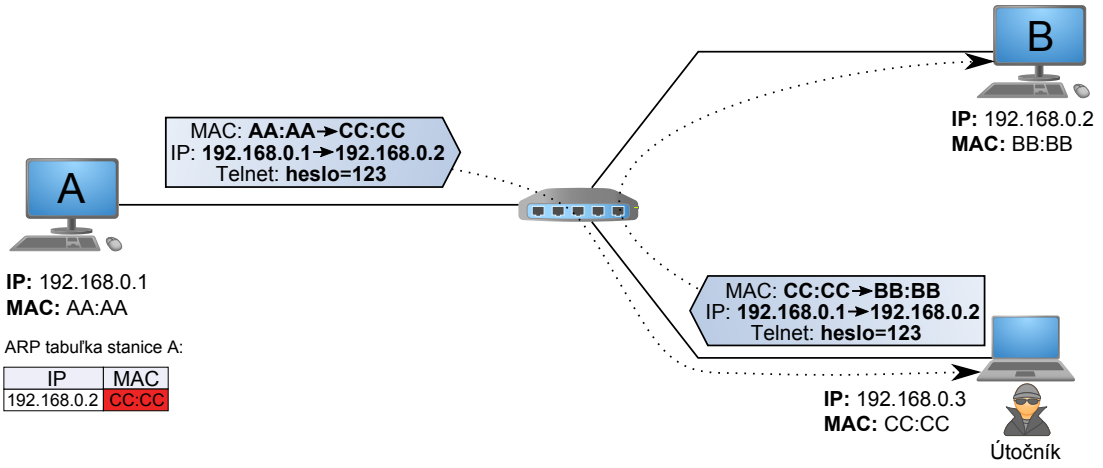
ARP spoofing je taktiež nazývaný ako ARP poisoning a pri svojej funkcii spolieha na neprítomnosť autentifikácie v ARP správach. V niektorých situáciach je to však výhodou, napríklad pri gratuitous ARP (gARP).
Funkcia gARP sa využíva, pokiaľ dve (primárne a sekundárne), poprípade viaceré zariadenia v sieti zdieľajú rovnakú IP adresu, no majú rozdielne MAC adresy. V prípade, že sa primárne zariadenie stane nedostupným, sekundárne ihneď odošle gARP správu pre každé zariadenie v sieti, aby informovalo, že majú používať jeho MAC adresu pre pakety využívajúce danú zdieľanú IP adresu. Táto situácia nastáva napríklad pri protokoloch ako sú VRRP alebo HSRP, ktoré slúžia na zlepšenie dostupnosti brány v sieti, respektíve spoľahlivosti, či rozloženia dátových tokov.

Hlavným cieľom útoku ARP spoofing je možnosť odpočúvať pakety posielané od jedného zariadenia k druhému. Útok pozostáva z posielania falošných nevyžiadaných paketov s ARP odpoveďami pre napádané zariadenie, v ktorých bude zmapovaná IP adresa druhého účastníka komunikácie, no MAC adresa útočníka. Tým pádom všetky pakety určené pre druhé zariadenie, sú posielané do útočníkovho zariadenia. Ten však po odchytení musí pakety preposlať ďalej druhému zariadeniu, inak sa komunikácia preruší a používatelia zaznamenajú chybovú situáciu. Útok však funguje len jednosmerne. Pokiaľ chce útočník odpočúvať trafiku aj od druhého zariadenia k prvému, musí poslať gARP pakety aj pre druhé zariadenie, aby si upravilo záznam v ARP tabuľke v jeho prospech.
Túto situáciu je možné využiť aj v prípade, že napádané zariadenie je smerovač. Útočníkovi tak bude umožnené odpočúvať pakety od všetkých staníc v danej všesmerovej doméne odosielané mimo ňu, napríklad do WAN, resp. internetu. Avšak

nebude môcť prijímať pakety, ktoré sú určené zo vzdialenej siete do jeho lokálnej siete len s jedným ARP spoofing útokom. Aby tieto pakety mohol odpočúvať, musí vykonávať niekoľko týchto útokov takým spôsobom, že vyšle niekoľko falošných ARP paketov priamo na smerovač s tým, že sa vydáva za všetky koncové zariadenia v sieti.[2, 5, 10, 11]



Obr. 3.3: Vyslanie falošnej ARP odpovede útočníkom. [2]



Obr. 3.4: Odpočúvanie paketov za pomoci útoku ARP spoofing. [2]

3.2.2 Detekcia útoku

Útok je možné detegovať buď na strane koncového používateľa, alebo na manažovateľnom prepínači.

O detekciu na strane používateľa sa stará personálny firewall, ktorý dokáže filtrovať ARP pakety. Dokáže rozpoznať napríklad veľmi vysokú intenzitu ARP odpovedí alebo situáciu, v ktorej zariadenie obdržalo ARP paket s odpoveďou, no nebol inicializovaný žiadnou ARP požiadavkou. V oboch prípadoch sú ARP pakety zahadzované. Pre bežne využívané operačné systémy (Windows, Linux) je k dispozícii mnoho aplikácií, ktoré monitorujú danú ARP tabuľku a pri jej zmene sú schopné upozorniť používateľa.

Na manžovateľnom prepínači je možné detegovať útok napríklad vypísaním ARP tabuľky, kde administrátor uvidí prepojenia medzi IP adresami, MAC adresami a príslušnými rozhraniami. [11, 2]

3.2.3 Ochrana voči útoku

Na strane používateľa, ako už bolo vyššie uvedené, sa stará o detekciu samotný firewall jeho zariadenia, taktiež sa stará o ochranu voči tomuto útoku tým, že nevyžiadané ARP pakety zablokuje. Avšak toto pravidlo neplatí v každej situácii. Niekedy nastáva problém pri rozlišovaní legitímnej funkcie ARP protokolu od škodlivej. Ďalšou možnosťou je používanie statických ARP záznamov, ktoré sú zadávané manuálne. Jedným zo spôsobov je vytvorenie dávkového súboru, v ktorom budú uvedené vopred definované statické údaje s tým, že pri každom spustení zariadenia ručne vymažeme záznamy v ARP tabuľke a použijeme dané statické záznamy z dávkového súboru.

Najkvalitnejšou ochranou voči ARP spoofing útoku je kontrola ARP paketov na prepínači. Tú však umožňujú až drahšie manažovateľné prepínače. Príkladom takejto funkcie je funkcia Dynamic ARP Inspection (DAI). Vyvinula ju firma Cisco v rámci bezpečnostných opatrení pre použitie do svojich prepínačov. DAI zabráňuje posielaniu neplatných ARP paketov v danej všesmerovej doméne, kontroluje celkovú ARP trafiku, ktorá prichádza na jeho rozhranie a zahadzuje rámce, ktoré nespĺňajú preddefinované pravidlá o prepojení IP adries s MAC adresami. Taktiež plní funkciu obmedzovania množstva ARP paketov, tým pádom ide aj o prevenciu pred DoS útokmi.

Ochrana voči útoku je možná aj na strane smerovača tým, že administrátor nastaví pevné prepojenie medzi IP adresou a MAC adresou. Tým sa zabráni odosielaniu rámcov zo smerovača na fiktívne (útočníkove) MAC adresy. Touto možnosťou však disponujú len drahšie, lepšie vybavené smerovače. [11, 2, 5, 3]

3.3 Port stealing

3.3.1 Charakteristika útoku

Port stealing, v preklade „kradnutie portu“, je útok, ktorého účel je podobný ako pri útoku ARP spoofing, kde sa útočník snaží získavať dáta, ktoré prebiehajú medzi komunikujúcimi koncovými stanicami.
Útočník si v prvom rade musí nastaviť sieťovú kartu do promiskuitného režimu a zistiť si MAC adresu obete. Tú si môže jednoducho zistiť za pomoci nástroja ARP ping (arping), ktorý je súčasťou mnohých softvérov určených pre monitorovanie siete, napr. *NetScanTools*. Aby však tento krok vykonal, musí vedieť IP adresu obete. ARP ping je podobný bežnému nástroju ping, avšak s rozdielom, že ping je súčasťou protokolu ICMP, ktorý pracuje na sieťovej vrstve OSI modelu, je smerovateľný a ARP ping využíva k svojej funkcii protokol ARP, ktorý pracuje na spojovej vrstve a nie je smerovateľný. Tým pádom je použiteľný len v rámci lokálnej siete.
Odpoveď na ARP ping môže mať podobu napríklad:

```
ARPING <IP adresa obete>
Reply from  <IP adresa obete>  <MAC adresa obete>  <čas odozvy>
Reply from  <IP adresa obete>  <MAC adresa obete>  <čas odozvy>
Reply from  <IP adresa obete>  <MAC adresa obete>  <čas odozvy>
Reply from  <IP adresa obete>  <MAC adresa obete>  <čas odozvy>
Sent 4 probe(s)
Received 4 response(s)
```

Útočník po zistení MAC adresy, ktorá prislúcha obeti, vyšle na prepínač rámce, v ktorých upraví zdrojovú MAC adresu na adresu obete. Cieľová MAC adresa v rámcoch bude patriť samotnému útočníkovi, takže sa fiktívne rámce nebudú odosielať na ďalšie rozhrania, tým pádom sa ostatné stanice pripojené k prepínaču nedozvedia o tejto situácii. Prepínač si následne opraví záznam v CAM tabuľke tak, že si bude myslieť, že obeť je pripojená k rozhraniu, ku ktorému je v skutočnosti pripojený útočník. Po tejto situácii nastáva spomínané „ukradnutie rozhrania“. Avšak pokiaľ sa v sieti nachádza viacej prepínačov, útočník môže cieľovú adresu v ním generovaných fiktívnych rámcoch nastaviť na všesmerovú, tým pádom sa rámce dostanú k obeti aj pokiaľ nie je pripojená práve na prepínač, na ktorom je útočník.
Následne rámec prechádzajúci cez prepínač od ľubovoľnej stanice k obeti bude obdržaný útočníkom. Ten ho môže buď analyzovať, alebo upraviť. Každopádne, pokiaľ nechce byť odhalený, musí rámec preposlať obeti, aby koncové stanice nezaznamenali chybovú situáciu. Aby však mohol rámec preposlať obeti, musí byť záznam v CAM tabuľke prepínača upravený. Útočník musí zastaviť odosielanie fiktívnych rámcov a vyslať rámec s ARP žiadosťou, ktorá bude určená pre IP adresu obeti, ktorá na

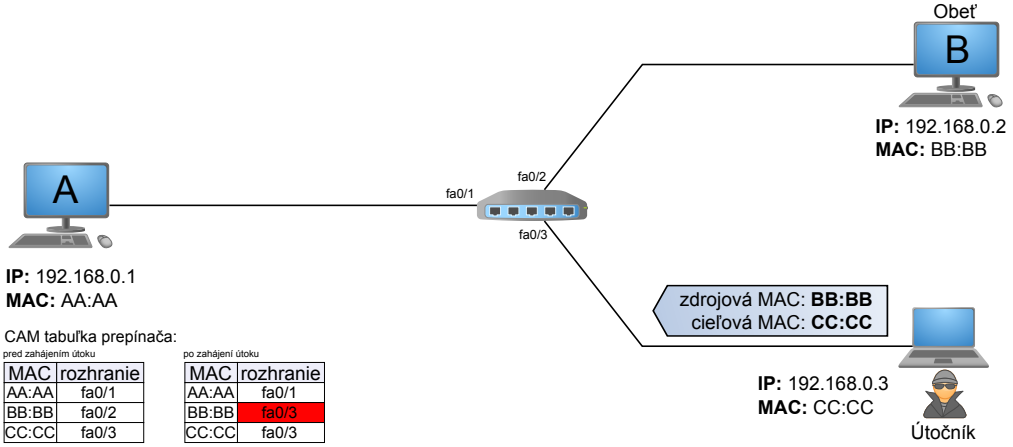
žiadosť odpovie ARP odpoveďou. Tým pádom si prepínač upraví záznam v CAM tabuľke a obeti priradí jej správne rozhranie. Keď útočník obdrží paket s ARP odpoveďou, má potvrdené, že CAM tabuľka má už korektný záznam a odchytený rámec jej môže preposlať. Útočník následne celý tento proces opakuje.
Útok však neprináša len výhody. Nevýhodou útoku je riziko, že pokiaľ obeť pošle počas útoku ľubovoľný rámec skorej ako útočník, záznam v CAM tabuľke prepínača sa upraví v prospech obete. Kvôli tomuto musí útočník zahlcovať sieť fiktívnymi rámcami s vysokou intenzitou a CAM tabuľka sa nestihne vždy v rýchlosti upraviť v prospech útočníka. [12, 10]

3.3.2 Detekcia útoku

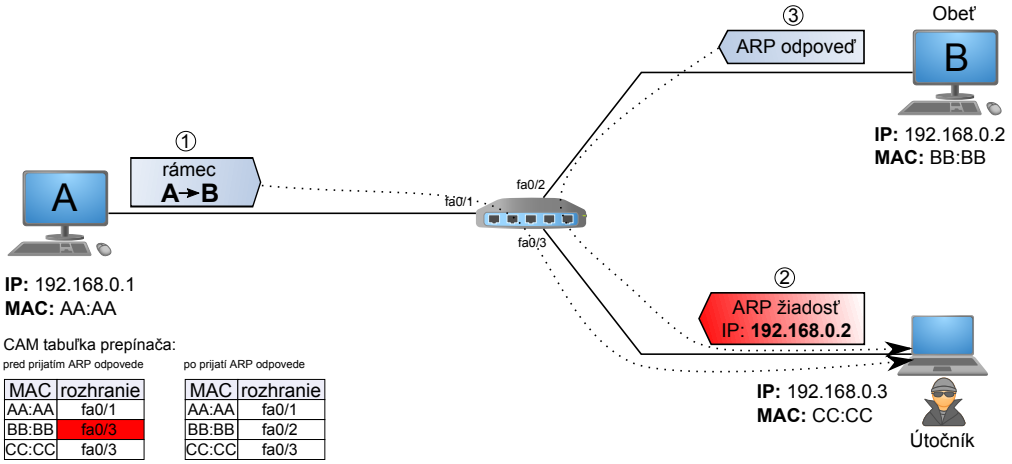
Útok je možno detegovať napríklad vypísaním CAM tabuľky na manažovateľnom prepínači.
Ďalšou možnosťou detekcie je pasívne monitorovanie sieťovej prevádzky. Pokiaľ administrátor zaznamená veľké množstvo rovnakých paketov s ARP žiadosťou, pravdepodobne sa jedná o útok. Obidva spôsoby detekcie boli popísané v časti 3.1.2. [12]

3.3.3 Ochrana voči útoku

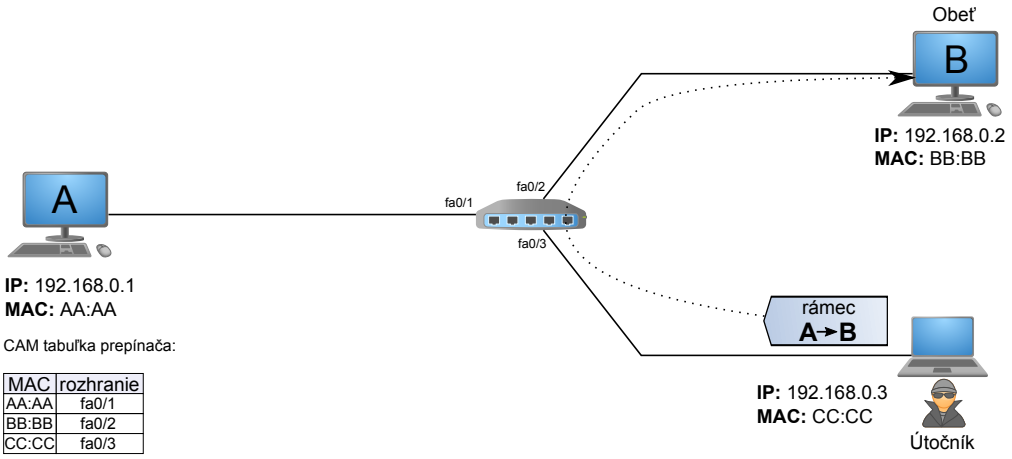
Ochranu je možné vykonať iba na drahších manažovateľných prepínačoch.
Jednou z účinných možností je zabezpečenie rozhrania, ktorá bola popísaná v časti 3.1.3.
Ďalšiu metódu ochrany predstavuje používanie statických ARP záznamov, ktoré sa vymažú z ARP tabuľky len za určitých podmienok. Táto metóda bola popísaná v časti 6.2.2. [12]



Obr. 3.5: Zahájenie útoku Port stealing fiktívnym rámcom.



Obr. 3.6: Odchytenie rámca útočníkom a následná oprava CAM tabuľky.



Obr. 3.7: Preposlanie pôvodného rámca obeti.

3.4 Útok na DHCP

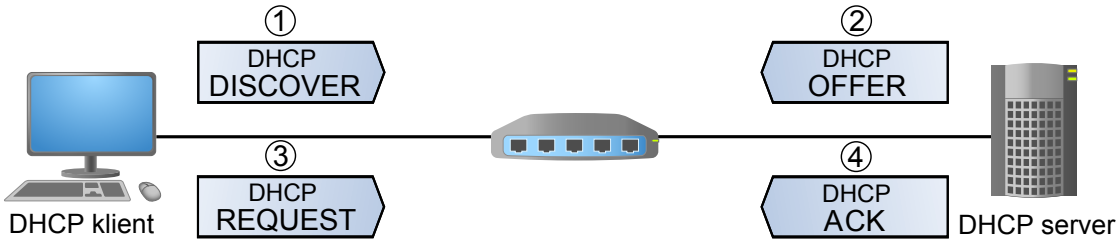
Dynamic Host Configuration Protocol – DHCP

Každé zariadenie v sieti, ktoré využíva sadu protokolov TCP/IP, potrebuje pre svoju komunikáciu platnú IP adresu. Pre niektoré zariadenia by mala byť IP adresa nakonfigurovaná staticky. Napríklad smerovače, prepínače, alebo servery využívajú statickú konfiguráciu. Výhoda tejto metódy je v tom, že nakonfigurovaná IP adresa môže na danom zariadení zotrvať na čas neurčitý. Napríklad pokiaľ využíva statickú konfiguráciu server, zariadenia jeho užívateľov po celý čas vedia, akou cestou sa k serveru dostanú z ľubovoľného miesta.
Avšak bežní koncoví užívatelia nemajú potrebu statickej konfigurácie, tým pádom serveru nezáleží na tom, že daný koncový užívateľ sa v prítomnom čase nachádza na jednej IP adrese, pričom sa v minulosti nachádzal na rozdielnej IP adrese. Koncoví užívatelia môžu mať IP adresu pridelenú dynamicky, aj keď sa postupom času zmení na inú.
Dynamické prideľovanie sieťových parametrov potrebných pre komunikáciu v sieti poskytuje koncovým užívateľom protokol **DHCP**. Okrem samotnej IP adresy sieťového rozhrania môžu klienti od DHCP servera obdržať aj masku siete, názov domény, východziu bránu, adresu DNS servera apod. Toto prideľovanie funguje na báze klient - server. Ako DHCP server môže figurovať napríklad smerovač, server, či počítač. Na jednej LAN sieti môže týchto serverov existovať niekoľko. To, od ktorého klient obdrží sieťové parametre, záleží od rýchlosti odpovede servera, poprípade od toho, či nemá server vyčerpané prideliteľné adresy. Rozlišujeme niekoľko základných typov DHCP paketov (správ):

- **DHCP discover** – objavenie (servera),
- **DHCP offer** – ponuka sieťových údajov,
- **DHCP request** – žiadosť o sieťové údaje,
- **DHCP ack** – potvrdenie,
- **DHCP decline** – odmietnutie pridelených sieťových údajov,
- **DHCP nak** – negatívne potvrdenie,
- **DHCP release** – vypustenie (IP adresy),
- **DHCP inform** – informovanie o udalosti.

Keď sa koncové zariadenie pripojí prvýkrát do siete, všesmerovo pošle paket **DHCP discover**. Tým informuje DHCP server(y), že sa nachádza v sieti. Pokiaľ sa DHCP server v sieti nachádza, reaguje na túto správu paketom **DHCP offer**, čím ponúka potrebné sieťové parametre. Klient pokračuje v komunikácii odoslaním paketu **DHCP request**, čím si vyžiada ponúkané parametre. Server na tento paket odpovedá správou **DHCP ack**, ktorým potvrdzuje klientovu žiadosť. Týmto procesom

klient obdržal potrebné sieťové parametre.
IP adresa však klientovi vydrží len určitý „čas prenájmu“ – anglicky lease time. Po vypršaní tohto času je stanica nútená k predĺženiu jej prenájmu. V prípade, že k tomuto nedôjde, DHCP server začne danú adresu ponúkať iným žiadajúcim zariadeniam, pretože ju považuje za voľnú.
Pokiaľ už zariadenie bolo niekedy v sieti pripojené, žiada DHCP server o jeho poslednú IP adresu, ktorú mu v minulosti pridelil, respektíve žiadá pomocou paketu **DHCP request**. Server buď klientovi vyhovie správou **DHCP ack**, alebo pridelí novú IP adresu z jeho rozsahu.
Každý klient, ktorý obdrží správu **DHCP ack**, by si mal ihneď overiť, či sa jemu pridelená IP adresa už nenachádza v sieti. Toto môže vykonať napríklad za pomoci ARP žiadosti. Pokiaľ klient zistí, že adresa sa už v sieti používa iným zariadením, pošle na server správu **DHCP decline**, čím odmietne pridelenú adresu a upozorní server na túto situáciu. Následne sa celý proces prideľovania opakuje.
Pokiaľ sa do siete pripojí zariadenie s už pridelenou IP adresu, ktorá sa buď v sieti používa iným zariadením, alebo je mimo adresný rozsah siete, DHCP server po zistení tejto nezrovnalosti informuje klienta negatívnym potvrdením – správou **DHCP nak**. V takejto situácií sa vykoná celý proces prideľovania odznovu s tým, že zariadenie obdrží nové sieťové parametre.
Môže však nastať situácia, keď daná stanica už IP adresu nepotrebuje. Vtedy klient pošle na server správu **DHCP release**, ktorou ho informuje o situácii a žiadá ho o uvoľnenie (deaktivovanie) jeho IP adresy.
V situácii, keď sa zariadenie, ktoré má napríklad manuálne nakonfigurovanú IP adresu pripojí do siete, klient vyšle správu **DHCP inform** pre server, a ten mu pridelí už len dodatočné sieťové parametre. [16, 15, 5]



Obr. 3.8: Grafické znázornenie procesu dynamického prideľovania sieťových parametrov protokolu DHCP.

3.4.1 Charakteristika útoku

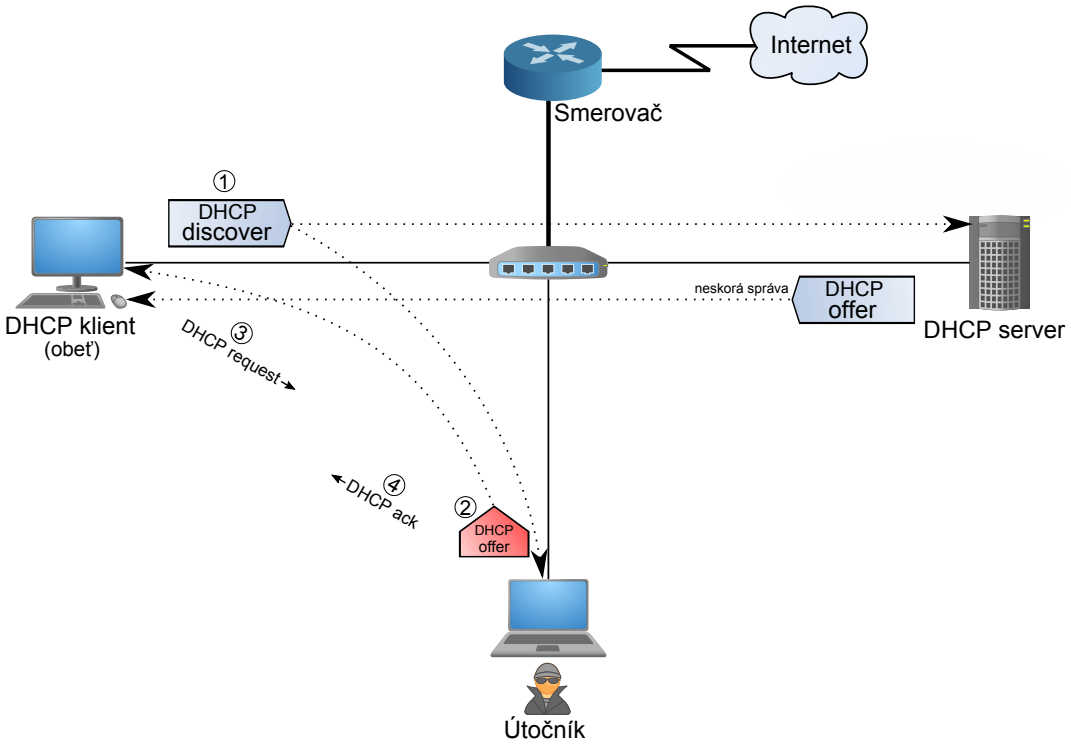
Na zneužitie protokolu DHCP budú popísané dva útoky. Prvým je *DHCP spoofing* (MITM útok), druhý nesie názov *DHCP starvation* (DoS útok).

DHCP spoofing

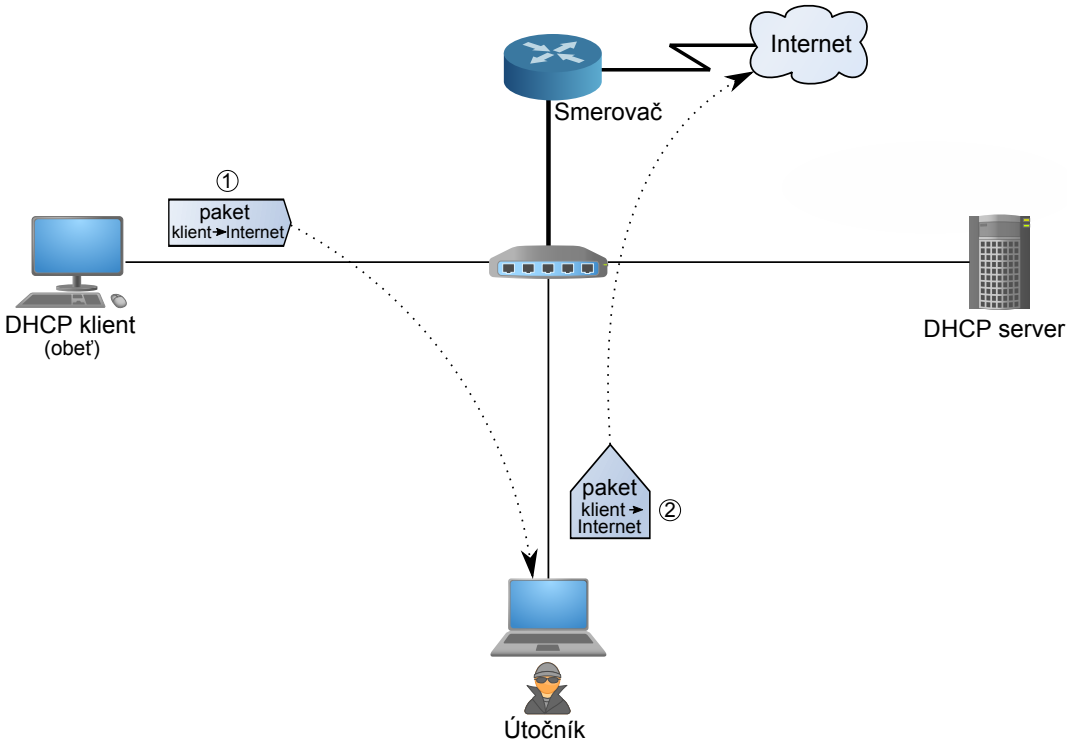
Princípom útoku DHCP spoofing je zneužitie procesu prideľovania sieťových parametrov pre koncové zariadenia, ktoré využívajú protokol DHCP.
Cieľom útočníka je dosiahnutie, aby klient (obeť) obdržal sieťové parametre od falošného DHCP servera, ktorý je spustený na útočníkovom počítači a nie parametre od legitímneho DHCP servera. Avšak nastáva otázka, ktorý DHCP server využije klient k prideleniu týchto parametrov? Pokiaľ klient obdrží niekoľko správ **DHCP offer** od niekoľkých serverov s tým, že v minulosti už bol pripojený do danej siete a server mu dokáže vyhovieť na požiadavku s klientom preferovanou IP adresou, použije tento server. Pokiaľ sa stanica pripojí do siete prvýkrát, záleží iba na tom, od ktorého DHCP servera príjme klient správu **DHCP offer** skorej. Túto situáciu útočník využije vo svoj prospech.
Hlavným princípom tohto útoku je podstrčenie fiktívnej adresy smerovača (brány). Týmto však útočník môže sledovať iba trafiku smerujúcu na túto bránu a nie aj v opačnom smere, pretože oklamaný bol iba klient, nie smerovač. Ten už posiela pakety priamo obeti. Táto situácia však útočníkovi stačí napríklad na odchytenie hesla služby HTTP, ktoré sa nachádza v pakete smerovanom od obeti do vonkajšej siete (internetu). [15, 3, 2]

DHCP starvation

Útok DHCP starvation spočíva v tom, že sa útočník snaží minúť všetky prideliteľné adresy DHCP servera. Túto situáciu dosiahne tak, že bude vysielať intenzívny prúd správ **DHCP discover** s náhodne vygenerovanými zdrojovými MAC adresami. Keďže server pri bežných nastaveniach nemá ako zistiť, či sa jedná o legitímne alebo fiktívne žiadosti, na tieto správy vyhovie. Pokiaľ budú po tomto procese klienti žiadať o IP adresu, DHCP server im už nebude môcť vyhovieť.
Keďže DHCP server musí každú požiadavku spracovať, existuje ďalšie riziko tohto útoku – vysoké zaťaženie CPU, čo vedie k výraznému spomaleniu jeho činnosti.



Obr. 3.9: Zahájenie útoku DHCP spoofing.



Obr. 3.10: Dôsledok útoku DHCP spoofing – presmerovanie trafiky na útočníkov PC.

3.4.2 Detekcia útoku

Jednou z možností detekcie je pasívne sledovanie siete. Spočíva v sledovaní situácie, kde na jednu správu **DHCP discover** zareaguje viacej DHCP serverov s odpoveďami **DHCP offer**. Ďalšiu situáciu môžeme spozorovať, ak má paket **DHCP offer** inú IP a MAC adresu ako legitímny DHCP server. V tomto prípade je veľmi pravepodobné, že legitímny DHCP server má už útočníkom vyčerpané prideliteľné IP adresy alebo je zahltený, takže už na žiadosti **DHCP discover** nereaguje.
Ďalšiu z možností predstavuje generovanie správ **DHCP discover** v pravidelných časových intervaloch s následným kontrolovaním ich odpovedí. Nevýhodou tejto možnosti je, že útočník dokáže ľahko rozpoznať vysokú intenzitu týchto paketov, pretože prichádzajú z jednej MAC adresy a následne ich môže zablokovať. [15]

3.4.3 Ochrana voči útoku

Najjednoduchšia možnosť ochrany voči útoku DHCP spoofing je nepoužívanie služby DHCP a konfiguráciu sieťových parametrov vykonať staticky manuálnym spôsobom. Táto možnosť je však nevhodná a neefektívna v prostredí väčších inštitúcii ako sú školy alebo firmy.
Ďalšia možnosť ochrany je, že pri použití DHCP servera bude nakonfigurovaný čo najdlhší čas prenájmu pre pridelené adresy. Táto možnosť je však tiež neefektívna predovšetkým vo väčších inštitúciach, kde nastáva časté pripájanie a odpájanie koncových zariadení.
Keďže útok DHCP starvation využíva k činnosti generovanie správ s náhodnými zdrojovými MAC adresami, je možné ako ochranu proti nemu použiť metódu zabezpečenia rozhrania, ktorá bola popísaná v časti 3.1.3.
Najsofistikovanejšiu ochranu voči útoku predstavuje mechanizmus *DHCP snooping*. [15, 3, 2]

DHCP snooping

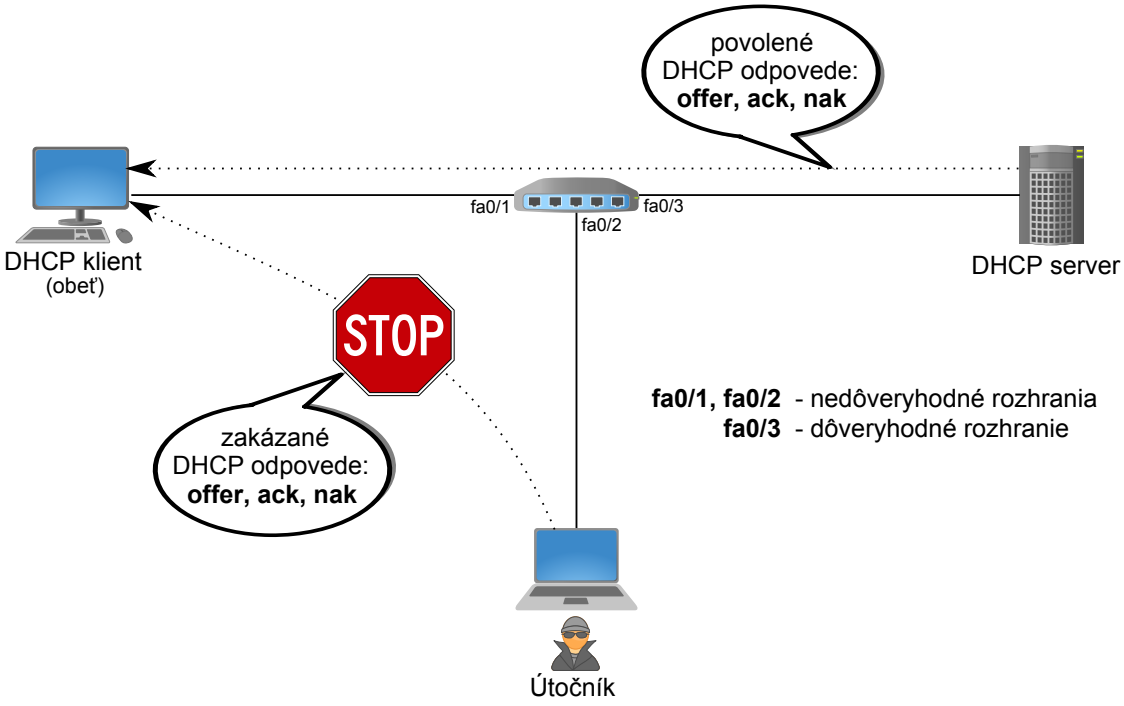
DHCP snooping predstavuje mechanizmus, ktorý sa zaoberá hĺbkovou kontrolou paketov počas operácie protokolu DHCP. Funkcia DHCP snooping je založená na označovaní rozhraní ako dôveryhodných (anglicky trusted ports) a nedôveryhodných (anglicky untrusted ports).
Koncové stanice, ktoré su pripojené do prepínača, nemajú žiadny dôvod generovať správy typu **DHCP offer** a **DHCP ack**; na obdržanie potrebných sieťových parametrov majú k dispozícii dostačujúce správy **DHCP discover** a **DHCP request**. Na základe tohto faktu pracuje bezpečnostný mechanizmus DHCP snooping. Ten

neprepustí nežiadúce správy (offer, ack) cez rozhranie, ktoré je označené ako nedôveryhodné, viď obr. 3.11.

Mechanizmus DHCP snooping spĺňa funkciu určitého špecializovaného firewallu, logicky umiestneného medzi dôveryhodné a nedôveryhodné rozhrania prepínača. Pri svojej funkcii dynamicky zhromažďuje údaje o prepojení jednotlivých IP adries s MAC adresami a dodatočnými informáciami pre každé zabezpečené rohranie. Tým, že prepínač nahliada do jednotlivých DHCP paketov, učí sa IP adresy, ktoré DHCP server pridelil daným klientom s unikátnymi MAC adresami na jednotlivých rozhraniach prepínača v lokálnej sieti. Toto prepojenie má tvar `<IP adresa, MAC adresa, čas prenájmu, rozhranie>`. Po tom, ako je tento záznam vytvorený, prepínač s ním porovnáva prichádzajúce DHCP správy. Pokiaľ informácie v danom pakete nesúhlasia so záznamom, je zahodený.

DHCP snooping poskytuje ďalšie funkcie ako:

- Limitovanie počtu DHCP správ na rozhraní v krátky časový okamžik,
- overovanie DHCP správ,
- poskytovanie informácii o tom, od ktorého prepínača a z akého rozhrania prišla DHCP žiadosť na server,
- prevencia proti DoS útokom v súvislosti s DHCP protokolom. [2, 15, 3]



Obr. 3.11: Funkcia mechanizmu DHCP snooping. [2]

3.5 VLAN hopping

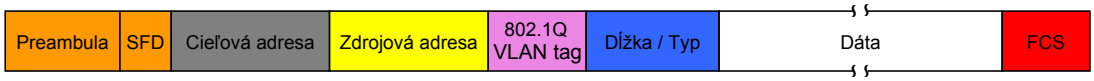
VLAN (Virtuálna LAN) slúži k logickému rozdeleniu lokálnej siete nezávisle na fyzickom usporiadaní. Každá VLAN predstavuje individuálnu všesmerovú doménu, tým pádom je charakterizovaná vlastným adresným priestorom.
Do jednotlivých VLAN môžu byť prideľované rozhrania či už individuálne, alebo skupinovo. Iba koncové zariadenia, ktoré sú pripojené do rozhraní patriacim pod jednu spoločnú VLAN, môžu spolu voľne komunikovať. Pokiaľ chce určité zariadenie komunikovať so zariadením nachádzajúcim sa v rozdielnej VLAN, je potrebné do topológie zaviesť zariadenie, ktoré je schopné pracovať na sieťovej vrstve OSI modelu. Týmto zariadením môže byť buď smerovač, alebo viacvrstvový prepínač.
Výhody zavádzania VLAN:

- **Kontrola všesmerovej trafiky** – v lokálnej sieti obdržia všesmerovú správu všetky zariadenia, no keďže každá jednotlivá VLAN predstavuje všesmerovú doménu, táto trafika sa nikdy nedostane za hranicu danej VLAN,
- **bezpečnosť** – VLAN siete umožňujú administrátorom logické oddelenie určitých skupín užívateľov. Táto možnosť je široko používaná v inštitučných sieťach ako sú firmy, školy apod., kde nastáva napríklad separácia manažmentu od IT oddelenia, separácia učiteľov od študentov atď.
- **flexibilita a rozšíriteľnosť** – koncové zariadenia môžu byť ľubovoľne premiestňované v rámci fyzickej siete a stále patriť do rovnakej VLAN.

V oblasti VLAN rozlišujeme dva typy rozhraní na prepínači:

- **Access port** – jedná sa o prístupové rozhranie, ktoré pridelené jednej VLAN. Tento typ rozrhania je určený pre pripojenie koncových zariadení ako sú počítače, tlačiarne apod. Zariadenie sa automaticky po pripojení do tohto rozhrania stáva členom danej VLAN,
- **trunk port** – predstavuje typ rozhrania, ktoré dokáže prenášať niekoľko VLAN sietí po jednom fyzickom médiu. Tento typ rozhrania sa využíva buď v spojoch medzi prepínačmi, alebo medzi prepínačom a smerovačom, ktorý vykonáva smerovanie medzi jednotlivými VLAN.

Pokiaľ je rozhranie v režime **trunk**, prepínač potrebuje určitý mechanizmus na to, aby identifikoval, do ktorej VLAN patrí ktorý rámec. Tento mechanizmus sa nazýva **frame tagging** (značkovanie rámcov) a do každého prepínačom prijatého rámca vloží 4bajtové pole **VLAN tag**, ktoré obsahuje pole VLAN ID (identifikátor VLAN, najčastejšie číslo). Toto značkovanie nastáva len v prípade, že daný rámec opustil trunkové rozhranie a odstránenie tagu nastáva v konečnej fáze prenosu, keď prepínač posiela rámec priamo pripojenému koncovému zariadeniu. Najčastejšie používaným štandardom pre značkovanie rámcov je **IEEE 802.1Q**, označovaný aj ako **dot1Q**.



Obr. 3.12: Základná štruktúra ethernetového rámca doplnená o pole VLAN tag.

Natívna VLAN (anglicky native VLAN) – predstavuje typ VLAN, ktorý sa nastavuje na trunkových rozhraniach. Trafika, ktorá je zaradená do natívnej VLAN sa pri prenose nijako neznačkuje, a taktiež prichádzajúca neoznačkovaná trafika sa zaraďuje do tejto VLAN. Z toho vyplýva, že pokiaľ do trunkového rozhrania pripojíme stanicu, ktorá nepodporuje **trunk** (napr. bežný PC), bude komunikovať v tejto VLAN. Natívna VLAN sa často zavádza pre VLAN určenú sieťovým administrátorom, poprípade pri zapojení IP telefónu, za ktorým sa nachádza počítač.
[17, 14, 3]

3.5.1 Charakteristika útoku

Cieľom útočníka pri útoku VLAN hopping, v preklade „poskakovanie po VLAN“, je preniknutie do VLAN siete, do ktorej nemá povolený prístup. V útoku sa využíva metóda značkovania 802.1Q. Jednou z možností je útok *Switch spoofing*, druhú predstavuje *Double tagging* (dvojité značkovanie).

Switch spoofing

Útočníkovým cieľom pri tomto útoku je vyjednanie trunkovej linky medzi jeho zariadením a prepínačom. Tým získa prístup ku všetkým povoleným VLAN sieťam v danej doméne. Aby túto situáciu dosiahol, využije absenciu zabezpečenia protokolu **DTP** (Dynamic Trunking Protocol). Jedná sa o protokol, ktorý bol vyvinutý firmou Cisco za účelom automatizácie procesu vyjednania trunkovej linky medzi ich prepínačmi. DTP uvádza rozhrania do niekoľkých režimov:

- **Auto** – rozhranie je ochotné stať sa trunkom, pokiaľ je rozhranie susedného zariadenia nastavené na režim *trunk* alebo *desirable*,
- **Desirable** – rozhranie sa stane trunkom, pokiaľ je rozhranie susedného zariadenia nastavené na režim *trunk*, *desirable*, alebo *auto*,
- **On** – rozhranie sa automaticky aktivuje do režimu trunk bez ohľadu na režim rozhrania susedného zariadenia, až kým nepríjme DTP správu, ktorá vyslovene deaktivuje trunk,
- **Nonegotiate** – DTP správy nie sú vysielané susednému zariadeniu. Pokiaľ má byť aktivovaná trunková linka, musí byť susedné rozhranie v režime *trunk*,

- **Off** – vyjednanie trunkovej linky nebude povolené bez ohľadu na režim rozhrania susedného zariadenia.

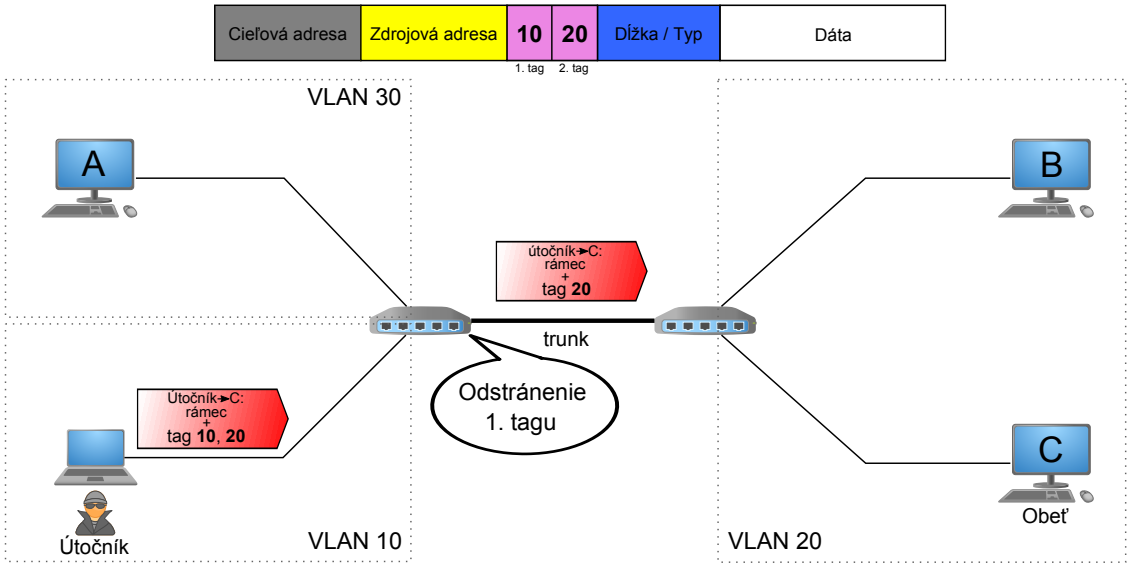
Predvolený režim rozhrania na Cisco prepínačoch je *desirable*, čo predstavuje pre danú sieť bezpečnostné riziko v prípade, že ho administrátor nechá v tomto režime. Útočník si tak môže vytvoriť vlastný DTP paket, ktorý odošle na toto rozhranie a tým si vyjedná trunk a zároveň prístup k VLAN sieťam. Po získaní tohto prístupu už môže vykonať rôzne MITM alebo DoS útoky.

Double tagging

Aby mohol byť útok uskutočnený, trunk na prepínači musí mať nastavenú rovnakú natívnu VLAN, aká je pridelená ľubovoľnému prístupovému rozhraniu na prepínači. S touto možnosťou sa útočník snaží injektovať trafiku z jednej VLAN do druhej bez použitia smerovača (resp. viacvrstvového prepínača). V dôsledku obídenia smerovača je útok jednosmerný, čiže útočník nebude môcť obdržať žiadnu odpoveď na pakety smerované obeti. To však nie je v tomto prípade útočníková starosť, pretože stále môže vykonať útok DoS zahltením zariadení v danej VLAN.

Princíp útoku podľa obr. 3.13 za predpokladu, že útočník sa nachádza vo VLAN **10**, ktorá je na prepínačoch nastavená ako natívna:

1. Útočník vyšle rámec s dvomi 802.1Q tagmi: **10** a **20**,
2. prvý (vonkajší) tag patrí útočníkovmu prístupovému portu do VLAN (**10**),
3. druhý (vnútorný) tag patrí prístupovému portu, ktorý prislúcha VLAN obeti (**20**),
4. rámec prechádza cez *Prepínač 1*, tu je klasifikovaný ako spadajúci pod VLAN **10**,
5. rámec je určený pre cieľovú MAC adresu, ktorá sa nachádza mimo trunk,
6. pretože natívna VLAN je nastavená na prepínačoch ako VLAN **10**, prvý tag je odstránený a rámec putuje po trunku ako neoznačený,
7. rámec stále obsahuje pole s tagom pre VLAN **20**,
8. rámec prichádza na *Prepínač 2* s tagom **20**, tým pádom ho prepínač klasifikuje, že patrí do VLAN **20** a následne ho pošle obeti na základe MAC adresy,
9. rámec je doručený obeti. [2]



Obr. 3.13: Proces útoku VLAN hopping. [2]

3.5.2 Detekcia útoku

Útok je veľmi ťažko detegovateľný, pretože z pohľadu zariadení zapojených do procesu sa nejedná o žiadnu škodlivú činnosť.
Pri výpadku spojenia (spôsobeného DoS útokom) by mal napadnutý užívateľ kontaktovať administrátora, ktorý následne skontroluje, či nastavená ochrana na prepínači zahŕňa aj ochranu voči tomuto útoku. [2]

3.5.3 Ochrana voči útoku

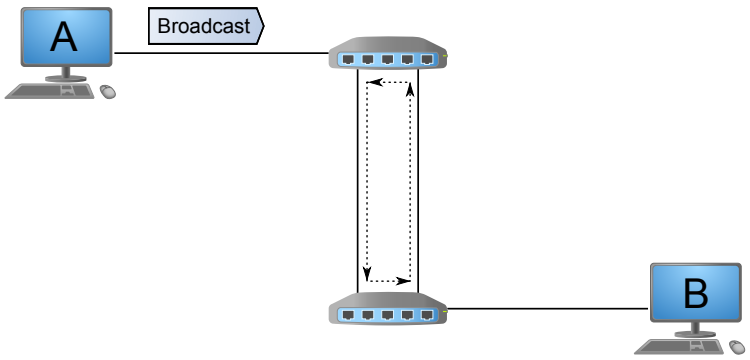
Ako ochrana proti útoku Switch spoofing je dostačujúca prevencia proti nemu. Administrátor by rozhrania nemal nechávať v žiadnom dynamickom režime. Namiesto toho je vhodné tieto rozhrania nastaviť do režimu *access*, teda prístupového režimu. V tomto režime všetky prijaté DTP správy budú zahodené, tým pádom pokusy o vyjednanie trunkovej linky budú neúspešné.

Proti útoku Double tagging by sa administrátor v prvom rade mal uistiť, že natívna VLAN nie je pridelená žiadnemu prístupovému rozhraniu. Tým pádom má útočník porušenú základnú podmienku pre vykonanie útoku.
Ďalšia možnosť ochrany je nepoužívanie natívnej VLAN. Táto možnosť je však nevhodná a jej použitie v praxi sa neodporúča.
Odporúčanou metódou ochrany je nakonfigurovanie prepínača, aby bola všetka trafika označovaná tagmi. Svojim spôsobom natívna VLAN stráca význam, avšak trafika posielaná z natívnej VLAN nie je nijako narušená, iba značkovaná. [2]

3.6 Útok na STP

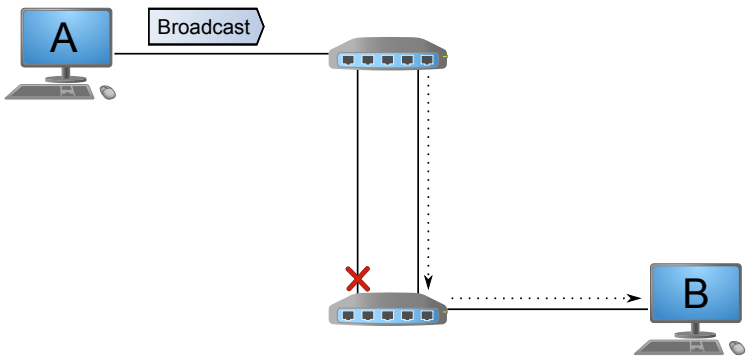
STP – Spanning Tree Protocol

Jedná sa o protokol, ktorý prepínačom umožňuje odhaliť prepínaciu slučku v topológii a následne pomocou určitého algoritmu túto topológiu spraviť logicky bezslučkovú.
Prepínacia slučka môže vzniknúť predovšetkým v dôsledku redundancie liniek medzi zariadeniami. Pod pojmom redundancia sa rozumie prepojenie dvoch (alebo viacerých) zariadení niekoľkými linkami medzi sebou za účelom zaistenia spoľahlivého prenosu dát v prípade, že primárna linka prestane fungovať.
Podľa obr. 3.14: počítač A vyšle všesmerový rámec priamo pripojenému prepínaču, ten ho prepošle spodnému prepínaču obidvomi linkami a následne spodný prepínač prepošle tento rámec počítaču B a naspať vrchnému prepínaču. Pretože v ethernetovom rámci neexistuje principiálne podobné pole ako je TTL (Time to Live) v IP pakete, bude tento všesmerový rámec preposielaný medzi zariadeniami donekonečna, respektíve až kým nebude jedno zo zariadení vypnuté alebo nenastane prerušenie jednej z liniek. Tento jav sa nazýva všesmerová búrka (anglicky broadcast storm).



Obr. 3.14: Redundantné zapojenie prepínačov bez prítomnosti protokolu STP. [2]

Takáto situácia je v lokálnej sieti veľmi neefektívna, pretože každý prepínač musí daný všesmerový rámec spracovať a následne ho znovu preposlať. To má za následok prílišné vyťaženie CPU jednotlivých prepínačov a môže byť ovplyvnená celková stabilita lokálnej siete.
Protokol STP rieši túto situáciu tým, že niektorú z liniek logicky zablokuje a tým pádom sa prepínacia slučka nevyskytne, viď obr. 3.15. Logicky zablokovaná linka však bude naďalej fungovať ako záložná v prípade, že primárna linka prestane fungovať.



Obr. 3.15: Redundantné zapojenie prepínačov s prítomnosťou protokolu STP. [2]

Prepínače, na ktorých je spustený Spanning Tree protokol spolu navzájom komunikujú za účelom vytvorenia obrazu STP topológie a následného logického zablokovania určitých rozhraní, pokiaľ sa v topológii vyskytla prepínacia slučka. Akonáhle si prepínače tento obraz vytvoria, sieť je **konvergovaná**.
Pri STP protokole spolu prepínače komunikujú na multicastovej báze pomocou takzvaných BPDU (Bridge Protocol Data Unit) správ, ktoré si medzi sebou posielajú každé 2 sekundy (východzia hodnota).

Pre vytvorenie bezslučkového prostredia v lokálnej sieti vykonáva STP následovné funkcie:

1. Zvolenie **Root Bridge** prepínača,
2. identifikovanie **Root Port**ov,
3. identifikovanie **Designated Port**ov,
4. logické zablokovanie určitých rozhraní.

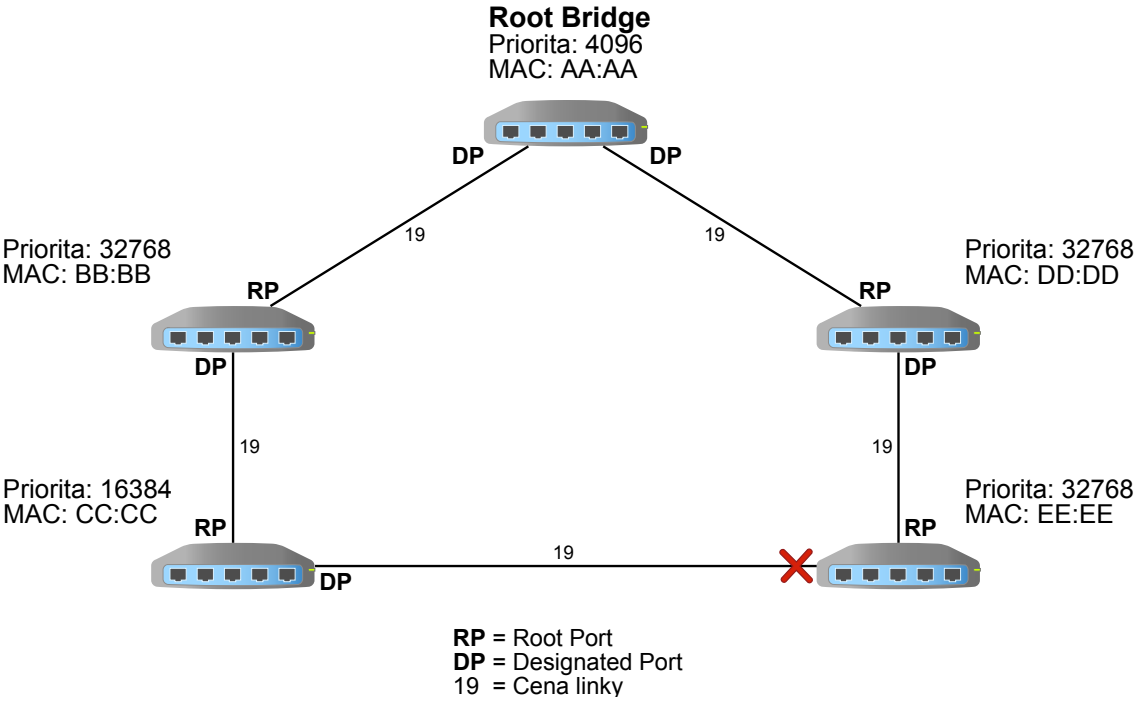
Zvolenie Root Bridge – tento proces spočíva v zvolení prepínača, ktorý sa javí ako centralizovaný bod v danej STP topológii. Root Bridge je zvolený na základe takzvného Bridge ID (BID). Bridge ID je kombinácia priority prepínača a jeho MAC adresy. Pokiaľ má prepínač v STP topológii **najnižšie** BID, stáva sa z neho Root Bridge.
Na začiatku STP procesu každý prepínač verí, že je Root Bridge, preto môže generovať BPDU správy. Pokiaľ prepínač obdrží od susedného zariadenia BPDU správu, porovná BID so svojou hodnotou, aby dokázal určiť, ktorý prepínač má túto hodnotu nižšiu. Iba prepínač s nižšou hodnotou môže naďalej generovať BPDU správy. Tento proces v topológii pokračuje, až kým nebude zvolený Root Bridge.

Identifikovanie Root Portov – každý prepínač, ktorý nie je Root Bridge, si zvolí jeden Root Port. Jedná sa o rozhranie, ktoré má najvhodnejšiu cestu k Root

Bridge prepínaču. Vhodnosť tejto cesty sa určuje na základe jej ceny (anglicky path cost). V závislosti ceny cesty a šírky pásma platí nepriama úmera – čím vyššia šírka pásma, tým nižšia cena a čím nižšia cena, tým je linka považovaná za vhodnejšiu. Ceny ciest:

- Ethernet = **100**,
- Fast Ethernet = **19**,
- Gigabitový Ethernet = **4**,
- 10gigabitový Ethernet = **2**.

Identifikovanie Designated Portov – každý sieťový segment vyžaduje určenie jedného Designated portu. Toto rozhranie má najnižšiu cenu cesty k Root Bridge prepínaču. Rozhrania na Root Bridge prepínači nemôžu byť blokované, preto sa z nich stávajú Designated Porty.



Obr. 3.16: Konvergovaná STP topológia. [17]

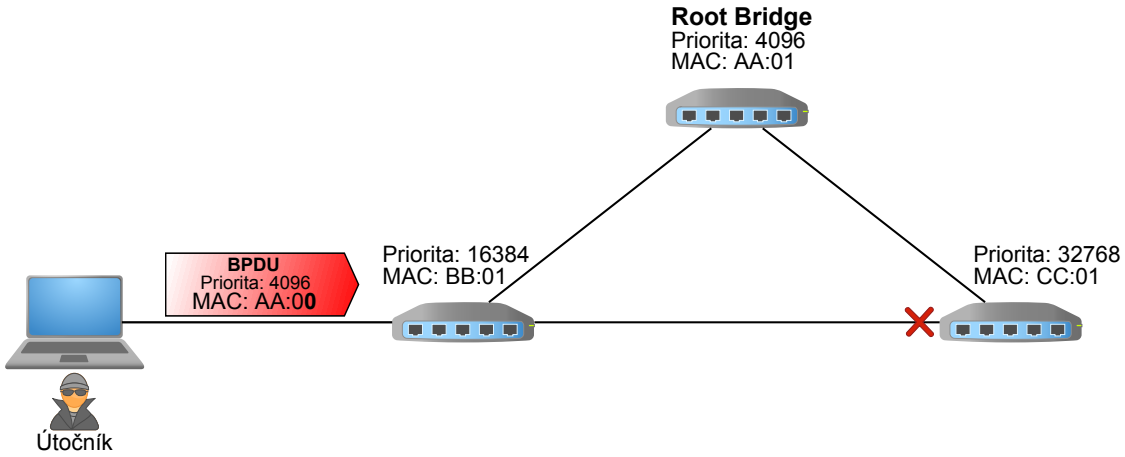
Na obr. 3.16 je znázornená konvergovaná STP topológia. Podľa vyššie uvedených procesov bol zvolený Root Bridge prepínač, Root Porty a Designated Porty. Cena cesty (Path Cost) sa v bežných situáciach využíva na určenie, ktoré rozhranie bude logicky zablokované. Avšak spodné prepínače majú cenu cesty k Root Bridge prepínaču rovnakú (*38*). Tým pádom, na prepínači, ktorý má najnižie BID, bude zvolený Designated Port a na prepínači s vyšším BID bude rozhranie zablokované. [2, 8, 17]

3.6.1 Charakteristika útoku

Útok na STP môžeme rozdeliť do dvoch hlavných častí: prevzatie role Root Bridge prepínača a zaplavenie BPDU rámcami.

Prevzatie role Root Bridge prepínača

Protokol STP je dôverčivý a neposkytuje žiadny autentifikačný mechanizmus, preto prepínače pri východziom nastavení akceptujú a spracujú falošné BPDU rámce od útočníka bez akýchkoľvek prekážok.
Akonáhle útočník zahájí útok, posiela atakovanému prepínaču každé 2 sekundy BPDU rámce s rovnakou prioritou akú má súčasný Root Bridge prepínač, avšak s mierne zníženou hodnotou MAC adresy, čo mu zaistí nižšiu hodnotu BID a tým víťazstvo v novej voľbe Root Bridge prepínača. Nástroj pre vykonanie útoku však dokáže vygenerovať aj BPDU rámec, ktorý obsahuje prioritu aj MAC adresu nastavenú na hodnotu 0, tým pádom má útočník isté víťazstvo vo voľbe nového Root Bridge prepínača, pretože žiadny prepínač takýto rámec vygenerovať nedokáže.



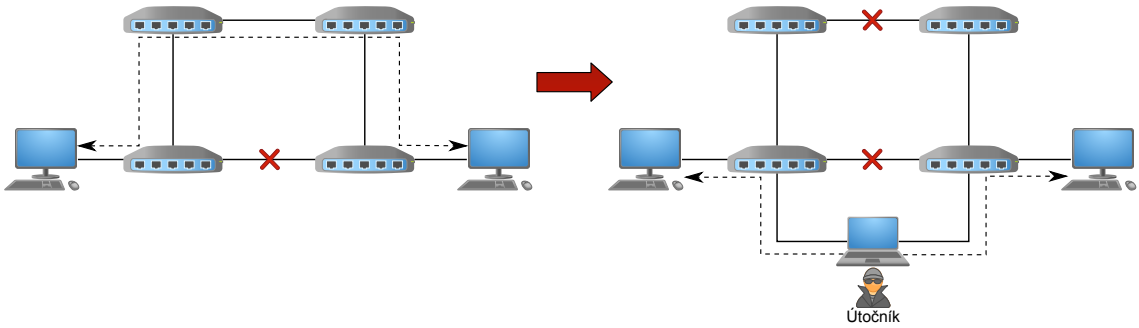
Obr. 3.17: Prevzatie role Root Bridge prepínača zaslaním falošného BPDU rámca.

Útočník má však po prevzatí role Root Bridge prepínača aj ďalšie možnosti.
Pokiaľ v STP topológii nastane zmena, napríklad zmena režimu rozhrania z blokovania do režimu posielania, daný prepínač vyšle pomocou svojho Root Portu smerom k Root Bridge prepínaču správu TCN BPDU (Topology Change Notification BPDU), ktorou ho o tejto zmene informuje. Na každú túto správu musí zainteresovaný prepínač zareagovať BPDU správou s nastaveným potvrdzovacím bitom TC-ACK. [2]

Útočník po prevzatí role Root Bridge prepínača môže v BPDU rámcoch nechať TC-ACK bit nenastavený, tým pádom bude neustále obdržiavať TCN BPDU správy,

na ktorých podnet musí informovať ostatné prepínače v STP topológii o jej zmenách. To má za následok skrátenie času životnosti záznamov v CAM tabuľke každého prepínača a následné nevyžiadané prúdenie rámcov v STP topológii. [2, 4]
Ďalšou možnosťou, ktorú má útočník po odoslaní BPDU rámca s nižším BID ako má Root Bridge prepínač, je následné zaslanie BPDU rámca s vyšším BID. Po tomto je nutné zvolenie nového Root Bridge prepínača, ktoré si vyžiadá určité zaťaženie CPU všetkých prepínačov v STP topológii. Pokiaľ sa táto akcia neustále opakuje, môže sa v konečnom dôsledku jednať o potenciálny DoS útok.

Druhým typom útoku pri prevzatí role Root Bridge Prepínača je takzvaná metóda Dual-Homed Switch. Jedná sa o útok typu MITM. Pre vykonanie tohto útoku musí byť útočníkov počítač vybavený dvomi ethernetovými sieťovými kartami. Na základe toho môže prijaté rámce odchytávať a preposielať ďalej smerom ku cieľu, viď obr. 3.18.



Obr. 3.18: Metóda Dual-Homed Switch pri útoku na protokol STP. [2]

Zaplavenie BPDU rámcami

Jedná sa o útok typu DoS, pri ktorom je útočníkovým cieľom jednoducho vyslať súvislý prúd BPDU rámcov na atakovaný prepínač, ktorý ich musí jednotlivo spracovať, až kým nie je jeho výpočtový výkon vyčerpaný. Nástroje ako Yersinia dokážu vygenerovať až niekoľko tisíc týchto rámcov za sekundu, čo je dostatočné množstvo na to, aby aj na výkonnom prepínači spôsobil zaťaženie CPU na 99 %.
Útočník má taktiež možnosť zaplaviť zariadenie TCN BPDU správami, ktorými núti Root Bridge prepínač, aby ich spracoval. Všetky ostatné prepínače v danej STP topológii zaznamenávajú v BPDU rámcoch nastavený TC bit a sú nútené k úprave času životnosti pri jednotlivých záznamoch v CAM tabuľkách.

3.6.2 Detekcia útoku

Detekcia útoku na protokol STP nie je jednoduchá, pretože z pohľadu samotného prepínača a protokolu STP sa nejedná o žiadnu škodlivú činnosť.
Zo strany administrátora sa dá útok detegovať na manažovateľnom prepínači tým, že si zobrazí počet prijatých BPDU rámcov. Pokiaľ bude tento počet príliš vysoký, jedná sa pravdepodobne o útok.
Ďalšou možnosťou je kontaktovanie administrátora koncovým užívateľom, ktorý zaznamená dlhší čas odozvy pri bežnej činnosti, poprípade výpadok komunikácie. Úlohou administrátora je následne skontrolovať vyššie uvedený počet prijatých BPDU rámcov, poprípade či celkové nastavenie STP protokolu odpovedá dokumentácii, alebo či je správne aplikovaná ochrana voči tomuto útoku.

3.6.3 Ochrana voči útoku

Root Guard

Pokiaľ je na touto funkciou zabezpečené rozhranie prijatý BPDU rámec s nižším BID ako má Root Bridge, je automaticky umiestnené do takzvaného *root-inconsistent* stavu, v ktorom nie je cezeň posielaná žiadna trafika. Aplikuje sa na Designated Porty a prepínač si na jeho základe udrží rolu Root Bridge.

BPDU Guard

Funkcia BPDU Guard zabezpečuje rozhrania prepínačov v STP topológii, ktoré sú určené pre koncových užívateľov. Zariadenia, ktoré sú pripojené do týchto rozhraní, napríklad útočník, nemôžu nijako ovplyvniť STP topológiu. Akonáhle je na takto zabezpečené rozhranie prijatý BPDU rámec, je ihneď umiestnené do takzvaného *err-disable* stavu. Inými slovami, je zablokované a prepínač vygeneruje správu pre administrátora, ktorá uvádza informáciu o narušení bezpečnosti.

BPDU Filter

Táto metóda ochrany zabráňuje posielaniu BPDU rámcov cez dané rozhranie v oboch smeroch. Jedná sa o typ ochrany ktorá je veľmi efektívna voči DoS útokom, pretože útočník pred zahájením útoku počúva BPDU rámce. Spomínaný mechanizmus mu v tejto činnosti zabráni. Avšak administrátor musí byť opatrný, na ktoré rozhranie túto ochranu aplikuje. Pokiaľ zvolí zlé rozhranie, môže narušiť celý STP proces a tým vzniknú prepínacie slučky, pretože BPDU Filtering je principiálne rovnaká funkcia ako vypnutie STP protokolu. [2]

4 POPIS PROGRAMOVÉHO VYBAVENIA

4.1 Kali Linux

Jedná sa o špecializovanú, voľne šíriteľnú Live CD distribúciu operačného systému Linux Ubuntu. Keďže sa jedná o live distribúciu, nie je nevyhnutná inštalácia systému na pevný disk, tým pádom sa dá spustiť z ľubovoľného bootovacieho média (CD, DVD, USB, . . .).
Pod pojmom Kali Linux sa rozumie operačný systém určený predovšetkým na testovanie sieťovej bezpečnosti. Obsahuje viac ako 300 bezpečnostných nástrojov a utilít, ktoré sú takisto voľne dostupné a niektoré ovládateľné aj v grafickom rozhraní. Medzi ne patria rôzne nástroje na testovanie bezpečnosti v lokálnych sieťach ako *Macof*, *Ettercap*, alebo *Yersinia*. Ďalej obsahuje aj nástroje ako *Aircrack-ng* (testovanie zraniteľností bezdrôtových štandardov), Cisco nástroje, skenery, nástroje na reverzné inžinierstvo, sieťové analyzátory ako *Wireshark* a mnoho iného. [18]

4.1.1 Macof

Macof je nástroj, ktorý je súčasťou sady Dsniff a je využívaný k nárazovému zaplaveniu prepínača rámcami. Nástroj Macof dokáže generovať až 155000 rámcov s náhodnými MAC adresami za minútu. To urobí z prepínača zariadenie funkciou podobné rozbočovaču a útočník môže následne odchytávať pakety. [19]
Zobrazenie manuálu nástroja je možné pomocou príkazu `#man macof`.

4.1.2 Ettercap

Ettercap je program, ktorý podporuje odpočúvanie paketov či už v káblovej, alebo bezdrôtovej lokálnej sieti – takzvaný LAN sniffer. Program disponuje štyrmi MITM nástrojmi ako je ARP poisoning, ICMP redirect, Port stealing a DHCP spoofing. Ettercap spája odpočúvanie sieťovej trafiky s mnohými pluginmi, dokáže odchytiť dáta aktívnych spojení, HTTPS heslá, taktiež zvláda filtrovanie trafiky a je plne konfigurovateľný. [20]
Zobrazenie manuálu nástroja je možné pomocou príkazu `#man ettercap`.

4.1.3 Yersinia

Yersinia je medzi používateľmi obľúbený sieťový nástroj určený na zneužívanie slabín mnohých sieťových protokolov ako je: STP, CDP, DTP, DHCP, HSRP, IEEE 802.1Q, IEEE 802.1X, ISL a VTP. [21]
Zobrazenie manuálu nástroja je možné pomocou príkazu `#man yersinia`.

5 POPIS POUŽITÝCH PREPÍNAČOV

V praktickej časti práce sa okrem iných zariadení budú vyskytovať prepínače od výrobcov Hewlett-Packard a Cisco, ktoré patria k najpoužívanejším prepínačom v prostredí inštitúcií.
Útoky budú vykonávané práve na tieto zariadenia.

5.1 HP ProCurve 2626

Jedná sa o manažovateľný prepínač pracujúci na spojovej vrstve OSI modelu. Pre pripojenie poskytuje 24 rozhraní typu Ethernet/Fast Ethernet, 4 rozhrania typu Gigabit Ethernet a jedno rozhranie typu RS-232 pre konzolové pripojenie. Jeho prepínacia kapacita činí 9,6 Gbit/s a CAM tabuľka ponúka priestor pre 8000 záznamov. Prepínač disponuje aj rôznymi ochrannými mechanizmami ako je port security, DHCP snooping, BPDU filtering, DAP (Dynamic ARP Protection) - obdoba DAI pri zariadeniach od firmy Cisco, a iné. Viac na [22].

5.2 Cisco Catalyst 2950

Cisco Catalyst 2950 je manažovateľný prepínač pracujúci na spojovej vrstve OSI modelu, ktorý disponuje 24 rozhraniami typu Ethernet/Fast Ethernet, 2 rozhraniami typu Gigabit Ethernet a jedným konzolovým rozhraním typu RJ-45. Ďalej ponúka prepínaciu kapacitu 8,8 Gbit/s a CAM tabuľka umožňuje 8000 záznamov.
Prepínač ďalej disponuje rôznymi ochrannými mechanizmami ako je BPDU guard, port security, 802.1x apod. [23]

Obr. 5.1: HP ProCurve 2626. [37]

Obr. 5.2: Cisco Catalyst 2950. [38]

5.3 Cisco Catalyst 2960

Taktiež ako u predchádzajúcich prepínačov sa jedná o manažovateľný typ, ktorý pracuje na spojovej vrstve OSI modelu. Poskytuje 24 rozhraní typu Ethernet/Fast Ethernet, 4 rozhrania typu Gigabit Ethernet a pre konzolové pripojenie jedno rozhranie typu RJ-45. Zariadenie disponuje prepínacou kapacitou 32 Gbit/s a CAM tabuľka poskytuje priestor pre 8000 záznamov
Medzi jeho ochranné mechanizmy patrí napríklad port security, DHCP snooping, BPDU Guard a iné. Viac informácií na [24].

5.4 Cisco Catalyst 3550

Jedná sa o manažovateľný viacvrstvový prepínač, ktorý okrem bežných prepínacích funcí podporuje aj základné funkcie smerovania. Medzi ne patrí napríklad podpora smerovacích protokolov, ale aj smerovanie medzi VLAN sieťami. Vďaka optimalizácií hardvéru zvláda tieto funkcie rýchlejšie a efektívnejšie ako smerovač. Zariadenie poskytuje 24 rozhraní typu Ethernet/Fast Ethernet a pre konzolové pripojenie jedno rozhranie RJ-45. Jeho prepínacia kapacita je 8,8 Gbit/s a CAM tabuľka ponúka priestor pre 8000 záznamov. Ďalej disponuje širšou ponukou bezpečnostných mechanizmov (napr. DAI) a QoS.
Viac informácií k dispozícii na [25].

Obr. 5.3: Cisco Catalyst 2960. [39]

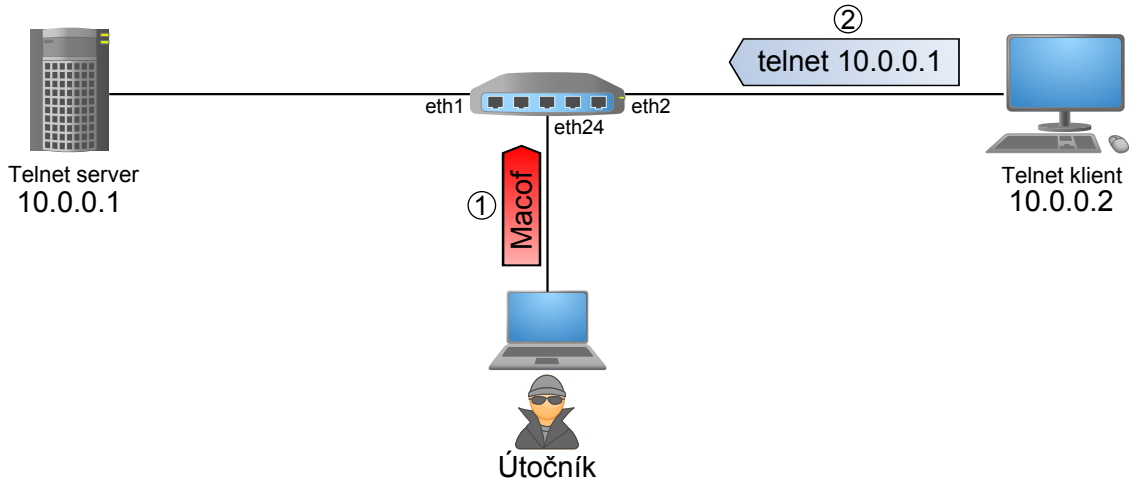
Obr. 5.4: Cisco Catalyst 3550. [40]

6 PRAKTICKÉ PREVEDENIE VYBRANÝCH ÚTOKOV

Všetky útoky budú vykonávané v laboratórnych podmienkach a zapojenia jednotlivých zariadení sa budú podľa možností snažiť o čo najautentickejšie principiálne napodobenie praktických situácií, ktoré môžu nastať v priestoroch rôznych inštitúcií.

6.1 MAC flooding

Na vykonanie tohto útoku bol použitý prepínač HP ProCurve 2626. Zapojenie je znázornené na obr. 6.1.



Obr. 6.1: Zapojenie pri útoku MAC flooding.

Ako už bolo uvedené v časti 3.1, cieľom útočníka je naplnenie CAM tabuľky prepínača, ktorý sa následne začne správať ako rozbočovač.
Útok však funguje len za určitých podmienok. Pokiaľ by útočník začal plniť CAM tabuľku prepínača v čase, keď sú doňho pripojené zariadenia, medzi ktorými chce trafiku odpočúvať, útok pravdepodobne úspešný nebude. Odpočúvanie nenastane, pretože prepínač si začne ukladať ďalšie záznamy pod už uložené záznamy, ktoré patria pripojeným zariadeniam. To znamená, že pokiaľ uvažujeme komunikáciu medzi týmito zariadeniami, prepínač bude vedieť, na ktoré rozhranie má daný rámec preposlať, a tak všesmerové preposielanie nenastane. Existuje však možnosť, že v určitom momente v prepínači daným zariadeniam vyprší v dôsledku nečinnosti časovač životnosti ich MAC adries a ten si ich záznamy následne vymaže z CAM tabuľky. Útočník vtedy môže využiť situáciu vo svoj prospech a CAM tabuľku naplniť. Táto situácia je však nepravdepodobná, predovšetkým pokiaľ sa jedná o zariadenie, na

ktorom je spustená služba, ku ktorej pristupuje denne mnoho ľudí a zároveň útočník nemá akým spôsobom zistiť, kedy tento moment nastane. Ďalšiu možnosť predstavuje fyzický prístup k atakovanému prepínaču. Pokiaľ by útočník získal fyzický prístup k prepínaču (napríklad pomocou sociotechniky), môže potrebné zariadenie odpojiť, následne prepínač reštartovať (kvôli vynulovaniu záznamov CAM tabuľky, ktorá je uložená v RAM pamäti prepínača) a po jeho nabootovaní útok vykonať. Pokiaľ po tomto úkone pripojí dané zariadenie do prepínača, všetky prijaté rámce určené preň budú posielané všesmerovo.
Pokiaľ však chceme útok vykonať efektívne, musíme túto akciu učiniť pre obidve odpočúvané zariadenia, aby sme komunikáciu odchytávali obojsmerne. Ak by sme v situácii na obr. 6.1 pred útokom odpojili iba Telnet klienta, odpočúvali by sme iba trafiku smerovanú k tomuto zariadeniu od Telnet servera. V tomto prípade by sa jednalo iba o odozvu, takzvané *telnet echo*, v ktorom síce nájdeme prihlasovacie meno, nie však heslo, viď obr. A.2 na ľavej strane. Pokiaľ by sme odpojili pred zahájením útoku iba Telnet server, prihlasovacie meno a heslo by sme síce odchytiť dokázali, no komunikácia, vzhľadom na to, že nie je obojsmerná, nebude kompletná. Viď obr. A.2 na pravej strane.

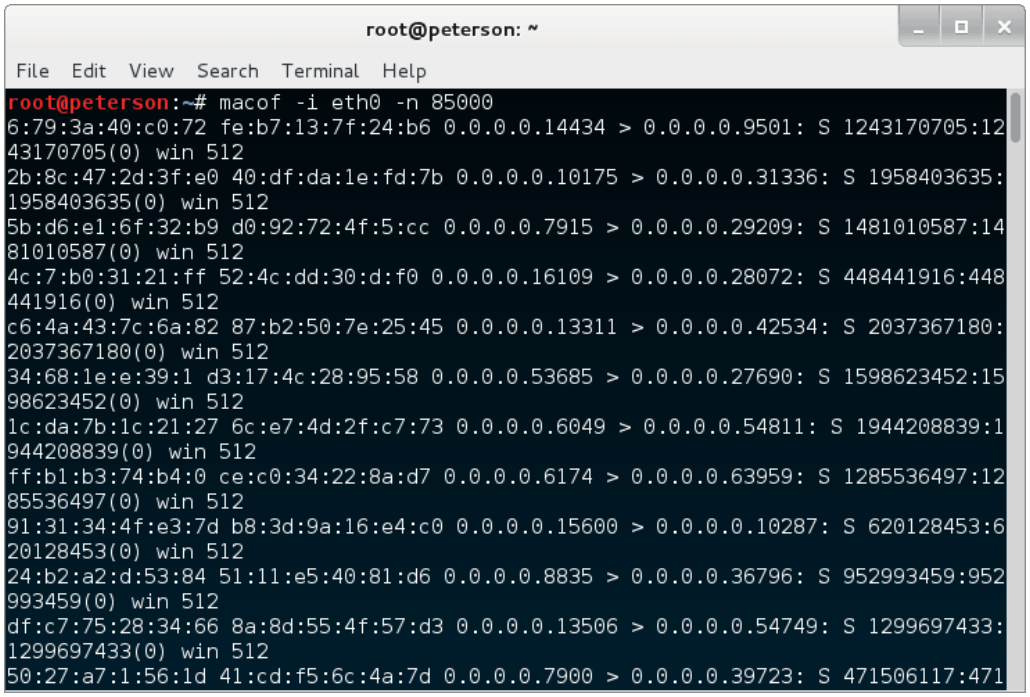
6.1.1 Vykonanie útoku

Pre praktické vykonanie útoku bola zvolená možnosť s odpojením zariadení a reštartovaním prepínača. Zariadenie, na ktorom bol spustený telnet server, je smerovač Cisco 2691, ktorý bol spustený na osobnom počítači v prostredí simulačného programu GNS3.

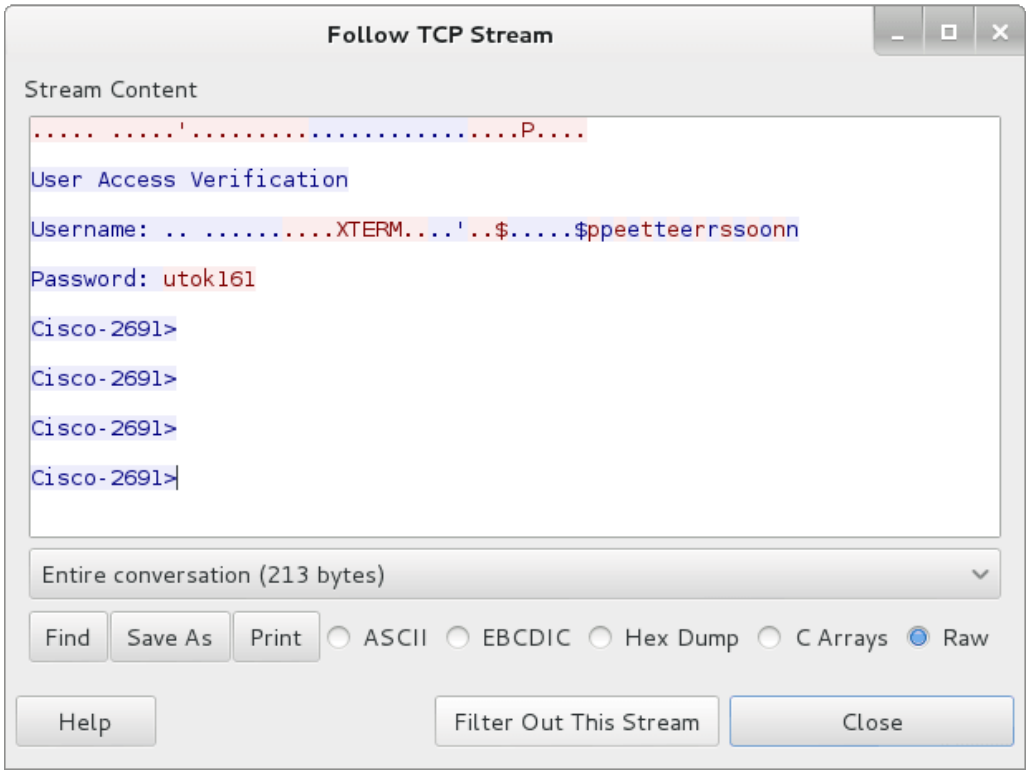
Pomocou príkazu zadaného v príkazovom riadku systému Kali Linux:

```
# macof -i eth0 -n 85000
```

spustíme nástroj Macof, za parametrom `-i` definujeme rozhranie, ktorým sa majú falošné rámce generovať a parametrom `-n` určíme počet týchto rámcov. To, že bola CAM tabuľka naozaj zaplnená môžeme vidieť na obr. A.3.
Po zapojení zariadení do prepínača bol klient prihlásený na Telnet server. Útočník mal spustený na svojom počítači sieťový analyzátor Wireshark, s ktorým túto komunikáciu odpočúval. Po obdržaní tejto komunikácie aplikoval filter „*telnet*“ a následne zvolil možnosť „*Follow TCP Stream*“, ktorou si zobrazil celý priebeh komunikácie, o ktorú mal záujem, viď obr. 6.3.
Dôvod, prečo je v prihlasovacom mene každé písmeno práve dvakrát je ten, že bola odchytená obojsmerná komunikácia, tým pádom sa do výsledku pričítali aj písmena, ktoré posielal Telnet server klientovi ako telnet echo.



Obr. 6.2: Zahájenie útoku MAC flooding.



Obr. 6.3: Zachytenie prihlasovacieho mena a hesla služby telnet.

6.1.2 Aplikácia ochrany voči útoku

Ako už bolo v časti 3.1.3 uvedené, vhodnou ochranou voči útoku je zabezpečenie rozhrania.
Rozhranie, ktoré bude zabezpečované je *ethernet 24*, na ktorom je pripojené zariadenie útočníka (v praxi samozrejme zabezpečujeme všetky rozhrania).
Na prepínač boli aplikované nasledovné príkazy:

```
ProCurve_2626(config)#port-security eth 24 learn-mode static
ProCurve_2626(config)#port-security eth 24 address-limit 3
ProCurve_2626(config)#port-security eth 24 action send-disable
```

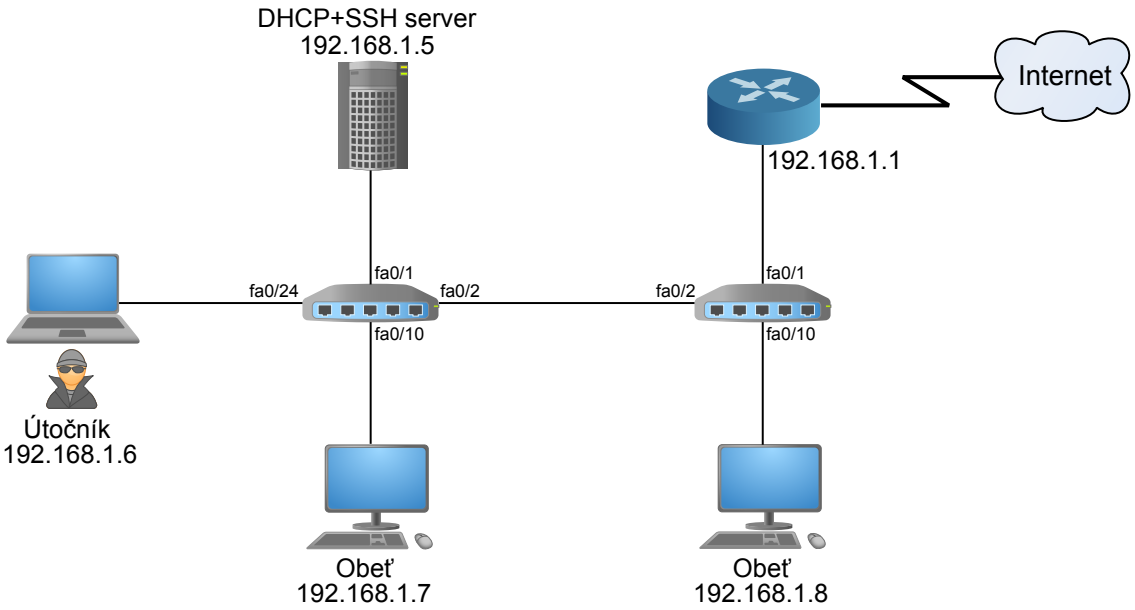
Pomocou kombinácie týchto parametrov bol prepínač nakonfigurovaný tak, že povolí na danom rozhraní maximálne 3 naučené MAC adresy a v prípade prečerpania tohto počtu pošle administrátorovi správu *SNMP Trap* a rozhranie zablokuje (vypne). Pre opätovné zapnutie rozhrania je nutný zásah administrátora, tým pádom nepomôže ani reštartovanie atakovaného prepínača.
Viac o zabezpečení rozhraní tohto prepínača k dispozícii na [26].

6.1.3 Vyhodnotenie útoku

Na základe podmienok popísaných v časti 6.1, za ktorých je útok vykonateľný a nutných úkonov zo strany útočníka, sa útok javí ako prakticky takmer nevykonateľný. Prepínač by však mal napriek tomu obsahovať konfiguračné opatrenia v podobe zabezpečenia rozhraní.

6.2 ARP spoofing

Útočníkovým cieľom pri útoku ARP spoofing je presmerovanie trafiky cez jeho zariadenie za pomoci nevyžiadaných ARP odpovedí, viď časť 3.2.1.
Na vykonanie tohto útoku boli použité prepínače Cisco C3550, DHCP a SSH server predstavuje smerovač Cisco 2691, ktorý bol nasimulovaný v prostredí programu GNS3. Zapojenie zariadení je znázornené na obr. 6.4. Útočník sa sústredil na odchytávanie prihlasovacích údajov nachádzajúcich sa v HTTPS a SSH trafike.



Obr. 6.4: Zapojenie pri útoku ARP spoofing.

6.2.1 Vykonanie útoku

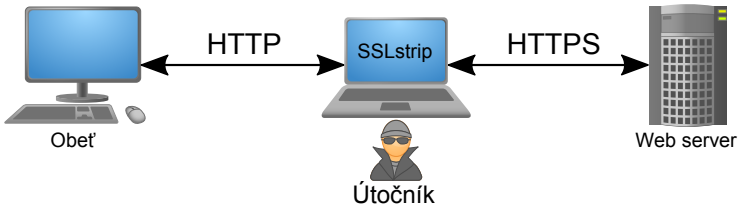
Odchytenie HTTPS

Na odchytenie údajov, ktoré sa nachádzali v HTTPS trafike útočník použil v systéme Kali Linux nástroj Ettercap a jeho textové rozhranie. Boli zadané nasledujúce príkazy:

```
# echo 1 » /proc/sys/net/ipv4/ip_forward
# iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 10000
# sslstrip -l 10000
```

Prvým príkazom sme aktivovali preposielanie prijatej trafiky od obete k cieľu a naopak. Druhým príkazom bolo aktivované presmerovanie portu 80 (HTTP) na port 10000. Na tomto porte naslúcha plugin SSLstrip (aktivovaný nasledujúcim príkazom).

Funkcia pluginu SSLstrip spočíva v tom, že pokiaľ je na útočníkovom zariadení zahájený MITM útok a zároveň tento plugin aktivovaný, tak HTTPS trafika smerovaná od servera ku klientovi bude po prechode útočníkovým zariadením degradovaná na HTTP trafiku, ktorá je následne ľahko odpočúvateľná, viď obr. 6.5.



Obr. 6.5: Komunikácia v prítomnosti pluginu SSLstrip.

Tento plugin necháme naďalej spustený a otvoríme si nové okno príkazového riadku, v ktorom zadáme už príkaz na samotné vykonanie útoku:

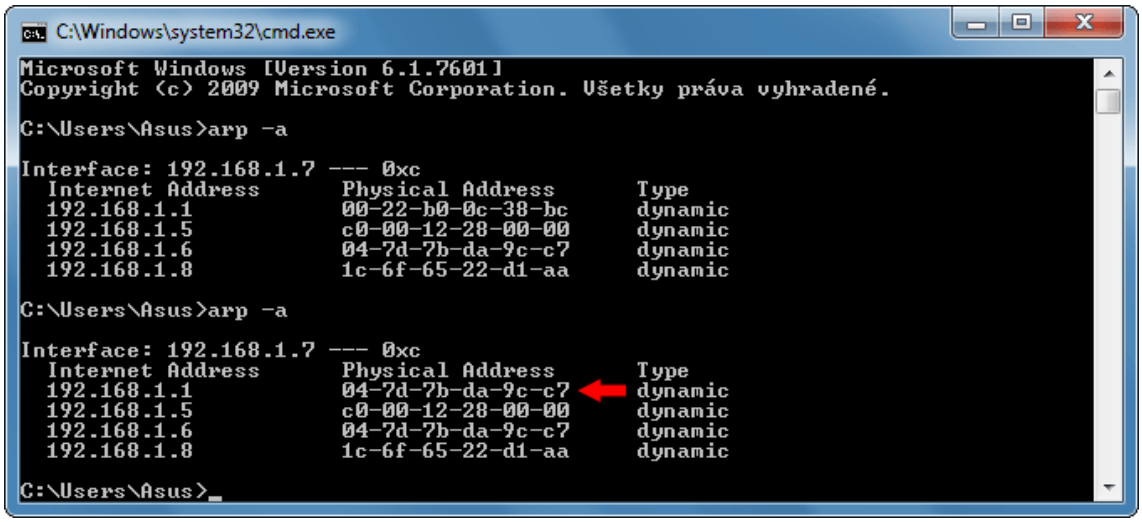
```
# ettercap -T -q -i eth0 -M arp:remote /192.168.1.7/ /192.168.1.1/
```

Parametrom `-T` definujeme, že sa jedná o textové rozhranie. Parametrom `-q` spustíme tichý režim (quiet mode), `-i` definuje rozhranie, ktorým je útočník pripojený do siete. `-M` definuje typ útoku MITM. Pomocou `arp:remote` definujeme útok ARP spoofing s účelom odpočúvania trafiky medzi koncovým zariadením a bránou. Pokiaľ by sme chceli odpočúvať trafiku len medzi koncovými zariadeniami, zvolíme parameter `arp:oneway`. Ďalej medzi prvými lomítkami definujeme IP adresu prvého cieľa – koncového zariadenia. Ako druhú uvádzame adresu brány. Pokiaľ by sme jednotlivé adresy nepoznali, necháme tieto parametre prázdne, čiže `// //`. Vtedy Ettercap odpočúva trafiku medzi všetkými zariadeniami v sieti.
Po potvrdení tohto príkazu je útok zahájený a ARP tabuľky „nakazené“. Viď obr. 6.6, kde je znázornená ARP tabuľka atakovaného zariadenia pred a po útoku. Obeť sa následne prihlasovala na stránky *paypal.com*, *gmail.com* a *vutbr.cz*. Tu však nastáva situácia, kedy rôzne webové prehliadače mali rôzne reakcie kvôli použitiu pluginu SSLstrip.

Tab. 6.1: Reakcie webových prehliadačov na plugin SSLstrip.

	IE v8-11	**Google Chrome** v34	**Mozilla Firefox** v29	**Opera** v21
Stránka	Reakcia	Reakcia	Reakcia	Reakcia
paypal.com	*	***	*	**
gmail.com	*	***	***	**
vutbr.cz	*	*	*	*

*** – prehliadač zablokuje prístup na stránku (obr. B.3),
** – prehliadač povolí prístup na stránku, no upozorní na bezpečnostné riziko (obr. B.2),
* – prehliadač neupozorní na bezpečnostné riziko a umožní prístup na stránku.



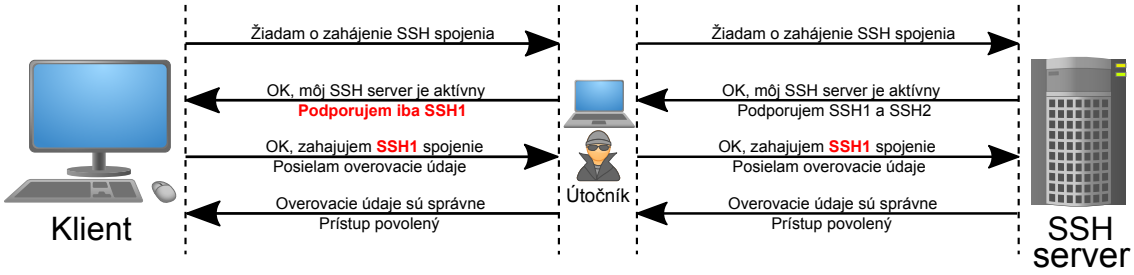
Obr. 6.6: ARP tabuľka atakovaného zariadenia pred a po útoku.

Na obr. 6.7 môžeme pozorovať výsledok útoku – odchytenie prihlasovacích údajov. V konkrétnom prípade sa obeť prihlasovala na stránku *paypal.com* pomocou prehliadača Mozilla Firefox.

Obr. 6.7: Odchytenie prihlasovacích údajov HTTP(S) komunikácie.

Odchytenie SSH

V dnešnej dobe množstvo používateľov nevedome využíva na vzdialený prístup k zariadeniam protokol SSH1, ktorý predstavuje oproti jeho nástupcovi, SSH2, výrazné bezpečnostné nedostatky, a tak je možné ho počas priebehu MITM útoku v dôsledku slabého autentifikačného mechanizmu v reálnom čase dekódovať a zaznamenať napríklad prihlasovacie údaje. Túto činnosť dokáže vykonávať aj nástroj Ettercap za pomoci jeho SSH filtra. Viac o rozdieloch medzi SSH1 a SSH2 dostupné na [27]. Pokiaľ má SSH klient nastavenú podporu oboch verzí protokolu (predvolené nastavenie klienta *Putty*), a taktiež SSH server podporuje obe verzie, poskytuje útočníkovi ideálnu situáciu na odchytenie prihlasovacích údajov. Proces degradácie protokolu SSH2 na SSH1 za uvedených podmienok môžeme sledovať na obr. 6.8.



Obr. 6.8: Grafické zobrazenie degradácie protokolu SSH2 na SSH1. [28]

Na vykonanie tohto útoku uvažujme situáciu z predchádzajúceho útoku, viď topológiu na obr. 6.4. Klient na adrese 192.168.1.8 sa pripája na SSH server za vyššie uvedených podmienok.
Útočník použil tentokrát grafické rozhranie nástroja Ettercap, v ktorom postupoval principiálne ako pri vyššie uvedenom spôsobe pomocou textového rozhrania a zahájil útok. Avšak s rozdielom, že zvolil parameter „*one-way*“ a nezvolil za svoje ciele konkrétne IP adresy, takže útočil na všetky zariadenia v sieti. Dodatočne je nutné spustiť SSH filter, ktorý sa nachádza v ponuke filtrov, no nevyhnutnosťou je jeho predchádzajúce skompilovanie. Proces degradácie počas vykonania útoku a následné odchytenie prihlasovacích údajov môžeme sledovať na obr. 6.9.

```
ARP poisoning victims:

 GROUP 1 : ANY (all the hosts in the list)

 GROUP 2 : ANY (all the hosts in the list)
Content filters loaded from /usr/share/ettercap/etter.filter.ssh.co...
[SSH Filter] SSH downgraded from version 2 to 1

SSH : 192.168.1.5:22 -> USER: peterson  PASS: utok161
```

Obr. 6.9: Proces útoku ARP spoofing pri odchytení údajov protokolu SSH.

6.2.2 Aplikácia ochrany voči útoku

Ako ochranný mechanizmus voči útoku bola použitá funkcia DAI, ktorej činnosť spočíva v hĺbkovej kontrole ARP paketov, kde sa zameriava na adresnú zhodu, ktorú overuje buď na základe záznamov vytvorených v databáze mechanizmu DHCP snooping, alebo pomocou staticky definovaných záznamov, takzvaných ARP prístupových zoznamov (anglicky ARP access control lists). Táto kontorola prebieha na

rozhraniach, ktoré sú určené ako nedôveryhodné a v prípade adresnej nezhody budú pakety zahodené. Ďalšou funkciou DAI je ochrana proti DoS útokom zablokovaním rozhrania v prípade prekročenia maximálneho počtu paketov za sekundu.

Keďže je v dnešnej dobe prítomnosť DHCP servera v sieti samozrejmosťou, omnoho jednoduchšiu možnosť v prípade väčších sieti predstavuje kontrola ARP paketov z databázy mechanizmu DHCP snooping. Pre konfiguráciu uvažujme schému z obr. 6.4.
Na ľavý prepínač boli aplikované nasledovné príkazy:

```
Cisco-C3550_L(config)#ip dhcp snooping
Cisco-C3550_L(config)#ip dhcp snooping vlan 1
Cisco-C3550_L(config)#interface fa0/1
Cisco-C3550_L(config-if)#ip dhcp snooping trust
```

Prvým príkazom sme globálne aktivovali mechanizmus DHCP snooping. Druhým príkazom sme definovali funkciu tohto mechanizmu pre VLAN 1, do ktorej patria všetky zariadenia pri predvolených nastaveniach. Následne sme zvolili dôveryhodné rozhranie, ktoré smeruje k DHCP serveru.
Pravý prepínač nakonfigurujeme obdobne, no ako dôveryhodné rozhranie zvolíme rozhranie smerujúce k DHCP serveru, čiže *fa0/2*.
Avšak nastáva problém s tzv. *Option-82*. Túto informáciu si prepínače vkladajú do DHCP správ a obsahuje identifikátory zariadení, pokiaľ je DHCP server v inej sieti ako klienti, ktorí si o údaje žiadajú. Option-82 je pri predvolených nastaveniach zapnutá, a pokiaľ sa DHCP server nachádza v rovnakej sieti ako klienti, smerovač nepridelí žiadané adresy, pretože v poli Option-82 nebude vyplnená adresa tzv. *relay agenta*, čo mu príde podozrivé. Preto je nutné na smerovač (DHCP server) aplikovať nasledovný príkaz:

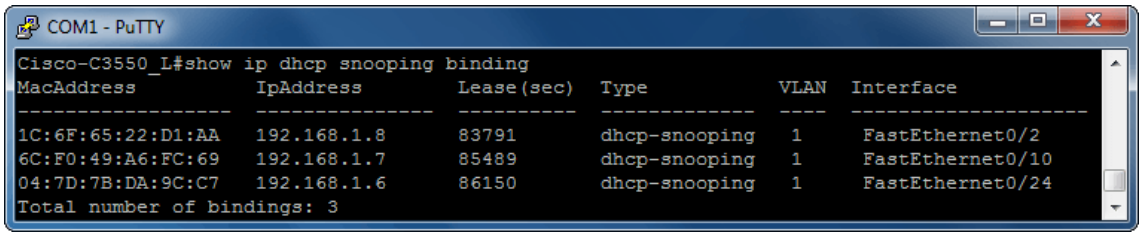
```
Cisco-2691(config)#ip dhcp relay information trust-all
```

Taktiež je nutné na oba prepínače aplikovať príkaz

```
Cisco-C3550(config)#ip dhcp snooping option allow-untrusted
```

Viac informácií o konfigurácii DHCP snooping a Option-82 k dispozícii na [29] a [30].

Tým je potrebná konfigurácia mechanizmu DHCP snooping ukončená a DHCP server dokáže prideľovať IP adresy, na základe čoho si DHCP snooping vytvorí svoju databázu. Viď obr. 6.10.



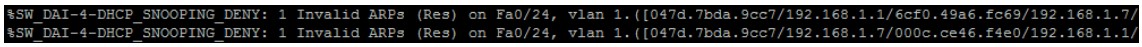
Obr. 6.10: Adresné prepojenie mechanizmu DHCP snooping na prepínači Cisco.

Nasleduje samotná konfigurácia mechanizmu DAI na ľavom prepínači:

```
Cisco-C3550_L(config)#ip arp inspection vlan 1
Cisco-C3550_L(config)#interface fa0/2
Cisco-C3550_L(config-if)#ip arp inspection trust
```

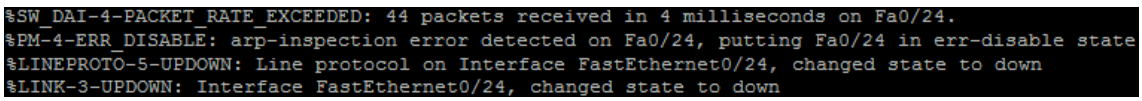
Pomocou týchto príkazov sme aktivovali DAI pre VLAN 1 a zvolili rozhranie *fa0/2* za dôveryhodné. Pravý prepínač bude nakonfigurovaný rovnako, pretože dôveryhodné rozhrania sa konfigurujú práve medzi prepínačmi. Na nich kontrola prebiehať nebude. Viac informácií o konfigurácii DAI k dispozícii na [31].

Útočník v prvom prípade (odchytenie HTTPS) zahájil útok s tým, že definoval jednotlivé ciele. Po zahájení mechanizmus DAI ihneď zareagoval výpisom na obr. 6.11 a následným zahodením paketov.



Obr. 6.11: Reakcia DAI na prvý útok.

V druhom prípade (odchytenie SSH) útočník nedefinoval konkrétne ciele, tým pádom Ettercap musel zmonitorovať, ktoré stanice sa nachádzajú na sieti. Tento úkon vykonal pomocou súvislého toku ARP žiadostí v celom adresnom rozsahu siete. ARP žiadosti nepredstavujú pre DAI riziko, preto na ne nezareagoval vyššie uvedeným spôsobom. Avšak DAI poskytuje aj ochranu proti DoS útokom, a tak mechanizmus zareagoval týmto spôsobom a rozhranie, ktorým tento prúd rámcov prijal, ihneď zablokoval, viď obr 6.12. DAI štatistiku môžeme sledovať na obr B.4.



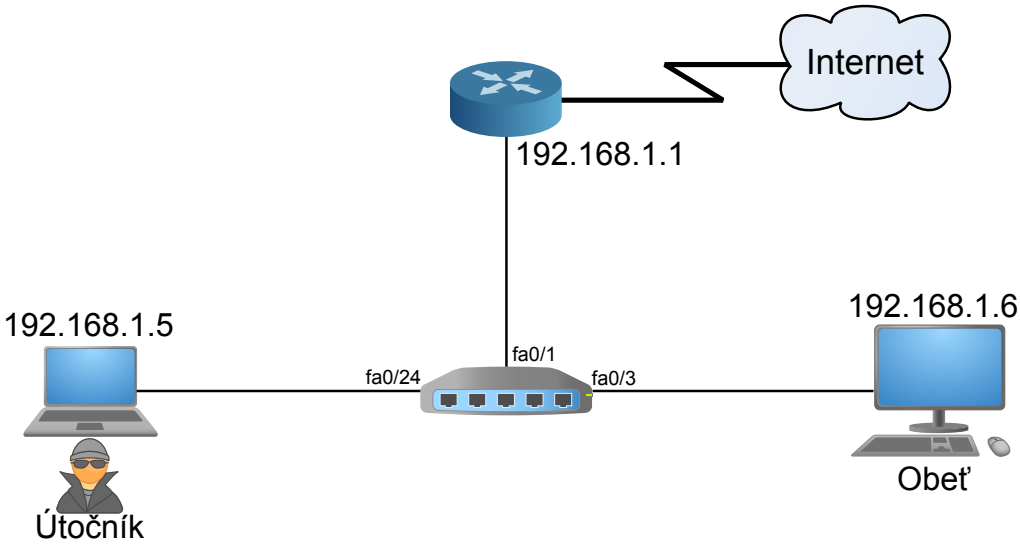
Obr. 6.12: Reakcia DAI na druhý útok.

6.2.3 Vyhodnotenie útoku

Podvrhnutím ARP protokolu v lokálnej sieti vzniká veľmi účinný obojsmerný MITM útok. Veľkou výhodou tohto útoku je jeho funkčnosť v rôznych podmienkach. Napríklad na rozdiel od útoku MAC flooding alebo DHCP spoofing, nepotrebuje k vykonaniu až také špecifické podmienky. Útočník dokáže presmerovať trafiku cez jeho zariadenie takpovediac „na požiadanie“. Ďalej je kompatibilný s rôznymi pluginmi a filtrami. Pomocou nástroja Ettercap sa dá vykonať ako v textovom, tak aj prehľadnom v grafickom rozhraní. Je relatívne jednoducho vykonateľný a pre bežného užívateľa, ktorý nemá na svojom počítači aktívnu ochranu práve proti ARP spoofingu, ťažko detegovateľný. Preto by sa mal o prevenciu proti nemu starať predovšetkým administrátor na aktívnych sieťových prvkoch a to napríklad mechanizmom DAI, ktorý dokáže útočníkovi radikálne znemožniť škodlivú ARP činnosť v danej sieti.

6.3 Port stealing

Útočníkovi sa pri tomto útoku jedná o presmerovanie trafiky cez jeho zariadenie za pomoci podvrhovania záznamov v CAM tabuľke prepínača. Pre popis útoku viď časť 3.3.1.
Zapojenie zariadení v sieti je znázornené na obr. 6.13 a ako centrálny prvok bol použitý prepínač Cisco C2960. Útočník použil grafické rozhranie nástroja Ettercap.



Obr. 6.13: Zapojenie zariadení pri útoku Port stealing.

6.3.1 Vykonanie útoku

Útočník zahájil útok v grafickom rozhraní nástroja Ettercap obdobne ako pri útoku ARP spoofing, no s rozdielom, že z ponuky MITM útokov vybral možnosť „*Port Stealing*“. Ďalej sa naskytujú dve možnosti: „*Sniff remote connections*“ a „*Propagate to other switches*“. Prvá možnosť predstavuje rovnakú funkciu ako pri útoku ARP spoofing, druhá možnosť je vhodná v prípade, keď chceme rozhranie „ukradnúť“ obeti, ktorá je pripojená v danej sieti do iného prepínača ako útočník. V tom prípade nebude cieľová MAC adresa rámca adresa útočníka, ale všesmerová.

Obr. 6.14: Možnosti útoku Port stealing.

Skutočnosť, že CAM tabuľka prepínača bola modifikovaná, si môžeme overiť jej zobrazením. Na Cisco prepínači je možné jej zobrazenie pomocou príkazu:

```
Cisco-2960#show mac address-table dynamic
```

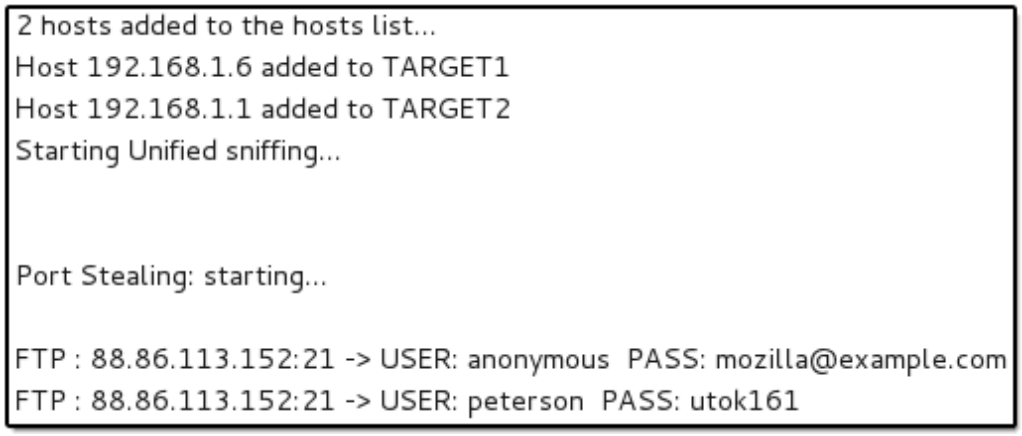
Parameter `dynamic` špecifikuje zobrazenie dynamicky naučených MAC adries. V prípade neuvedenia tohto parametru budú zobrazené aj statické MAC adresy, ktoré sú rezervované napríklad pre CPU prepínača. Výpis pred a po zahájení útoku je znázornený na obr. 6.15, z ktorého môžeme vidieť, že rozhrania, do ktorých je pripojený počítač obete a brána, sú „ukradnuté“.

```
1    000c.ce46.f400   DYNAMIC     Fa0/1
1    6cf0.49a6.fc69   DYNAMIC     Fa0/3
1    047d.7bda.9cc7   DYNAMIC     Fa0/24
```

```
1    000c.ce46.f400   DYNAMIC     Fa0/24
1    6cf0.49a6.fc69   DYNAMIC     Fa0/24
1    047d.7bda.9cc7   DYNAMIC     Fa0/24
```

Obr. 6.15: CAM tabuľka prepínača pred a po zahájení útoku Port stealing.

Obeť sa následne prihlásila do služby FTP. Odchytenie prihlasovacích údajov môžeme vidieť na obr. 6.16.



Obr. 6.16: Odchytené prihlasovacie údaje pomocou útoku Port stealing.

Obr. C.1 umiestnený v prílohe zachytáva priebeh tohto útoku v programe Wireshark. Z obrázku môžeme vidieť súvislý tok ARP rámcov, v ktorých útočník striedavo menil zdrojové MAC adresy obete a brány za účelom modifikácie CAM tabuľky prepínača. Taktiež môžeme vidieť odchytený paket služby FTP, ktorý momentálne prenáša prihlasovacie meno. Prvou červenou šípkou je znázornená ARP žiadosť, ktorú útočník poslal s dotazom na MAC adresu prislúchajúcu IP adrese brány. Tá mu na žiadosť odpovedala, tým pádom si prepínač opravil záznam v CAM tabuľke. Útočník následne odpoveď obdržal (druhá červená šípka) a tým vedel, že potrebný záznam v CAM tabuľke je korektný a odchytený FTP paket preposlal smerom k jeho cieľu.

6.3.2 Aplikácia ochrany voči útoku

Ideálnu ochranu voči útoku Port stealing predstavuje zabezpečenie rozhraní. Na prepínač boli aplikované nasledovné príkazy:

```
Cisco-2960(config)#interface fa0/24
Cisco-2960(config-if)#switchport mode access
Cisco-2960(config-if)#switchport port-security
Cisco-2960(config-if)#switchport port-security maximum 1
Cisco-2960(config-if)#switchport port-security mac-address sticky
Cisco-2960(config-if)#switchport port-security violation restrict
```

Prvým príkazom sme vstúpili do konfiguračného režimu rozhrania. Druhý príkaz uvedie rozhranie do prístupového režimu. Tretím príkazom aktivujeme funkciu zabezpečenia rozhrania. Ďalším príkazom definujeme maximálny počet bezpečných

MAC adries. Nasledujúcim príkazom definujeme dynamické naučenie autorizovaných MAC adries. Pokiaľ nepoužijeme parameter `sticky`, musíme nadefinovať MAC adresu manuálne. Posledný príkaz určuje, akú akciu prepínač vykoná v prípade porušenia bezpečnosti. Parameter `restrict` znamená, že po porušení tejto podmienky budú pakety zahodené, ďalej bude poslaná správa SNMP trap, zobrazí sa syslog správa a inkrementuje sa hodnota v počítadle bezpečnostných porušení. Ďalšiu možnosť predstavuje parameter `protect`, ktorý v prípade narušenia bezpečnosti nebezpečné pakety zahodí bez akéhokoľvek oznámenia. Poslednou možnosťou je parameter `shutdown`, ktorý dané rozhranie zablokuje (err-disable). V reálnej situácii je však vhodné zabezpečiť všetky prístupove rozhrania.
Viac informácií o zabezpečení rozhraní na tomto prepínači k dispozícii na [32].
Syslog správu o narušení bezpečnosti môžeme vidieť na obr. 6.17. Vo výpise sa striedajú dve konkrétne MAC adresy. Jedná sa o MAC adresy cieľov útočníka (obeť a brána), ktoré umiestňoval ako zdrojové vo vysielaných rámcoch.

Obr. 6.17: Syslog správa o narušení bezpečnosti pri zabezpečení rozhrania.

6.3.3 Vyhodnotenie útoku

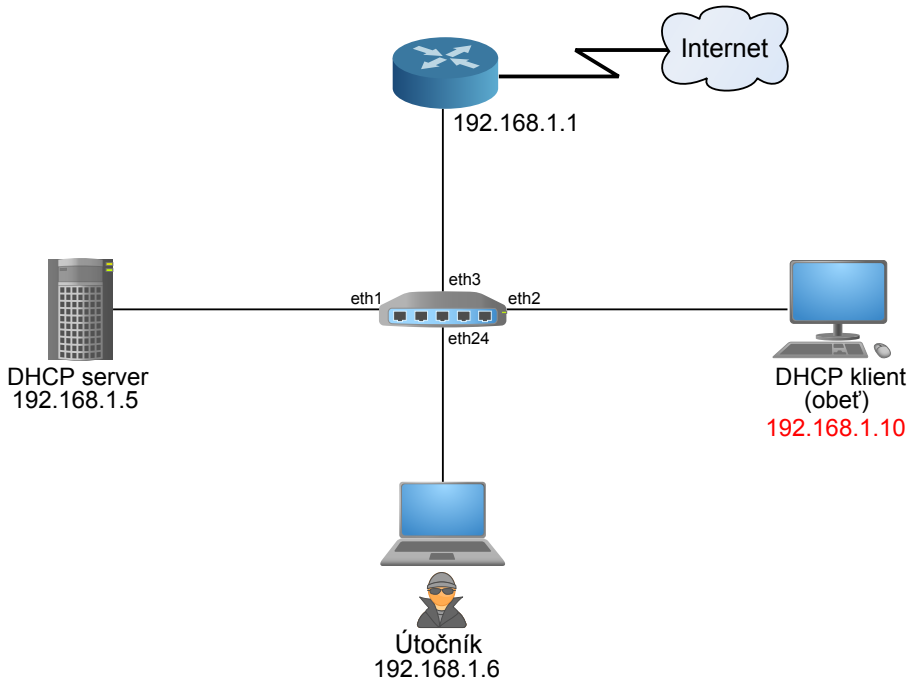
Sústavným modifikovaním CAM tabuľky prepínača podľa vyššie uvedených spôsobov vzniká obojsmerný MITM útok. Port stealing sa môže použiť napríklad v situácii, keď je na sieti aplikovaná ochrana proti útoku ARP spoofing (statické ARP záznamy, DAI, ...). Nevýhodou tohto útoku je neustále prúdenie rámcov, ktorými útočník modifikuje záznamy v CAM tabuľke, a tak môže vzniknúť situácia, v ktorej si prepínač nestihne (resp. nedokáže) tieto záznamy upraviť v prospech útočníka, čo bude mať za následok neodchytenie prenášaného paketu.

6.4 Útok na DHCP

6.4.1 Vykonanie útoku

DHCP spoofing

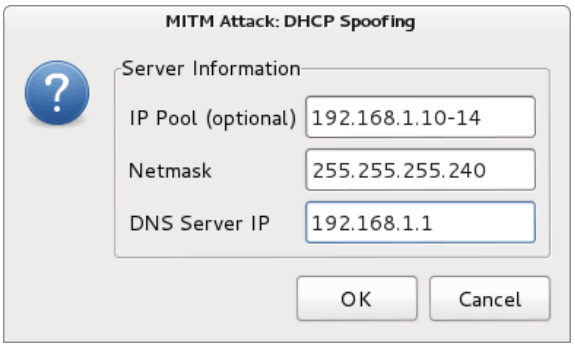
Ako bolo uvedené v časti 3.4.1, cieľom útočníka je, aby jeho obeť obdržala podvrhnuté sieťové údaje od ním vytvoreného falošného DHCP servera. Jedná sa hlavne o adresu brány, ktorú podvrhne za svoju adresu a tým presmeruje trafiku od klienta smerom k jeho zariadeniu. Tým vznikne jednosmerný MITM útok.
Na vykonanie tohto útoku bol použitý prepínač HP ProCurve 2626 ako atakované zariadenie. Útočník využíval grafické rozhranie nástroja Ettercap spustené v systéme Kali Linux. Ako DHCP server bol použitý smerovač Cisco 2691, ktorý bol nasimulovaný v prostredí programu GNS3.



Obr. 6.18: Zapojenie pri útoku DHCP spoofing.

Zapojenie zariadení do prepínača je znázornené na obr. 6.18. Sieť má vyhradený adresný priestor **192.168.1.0/28**. To znamená, že počet prideliteľných IP adries pre zariadenia je 14. DHCP server je nakonfigurovaný, aby prideľoval adresy v rozsahu 192.168.1.6 – 14.

Útočník po vybratí *DHCP spoofing* z ponuky MITM útokov musí nastaviť v nástroji Ettercap potrebné údaje, viď obr. 6.19.



Obr. 6.19: Nastavenie údajov pri útoku DHCP spoofing.

Ako prvé je potrebné nastaviť parameter *IP Pool*. Jedná sa o rozsah adries, ktoré bude útočníkov falošný DHCP server ponúkať svojim obetiam. Aj keď je tento parameter voliteľný, je vhodné ho nastaviť. Nástroj Ettercap však nekontroluje, či je už adresa z daného rozsahu pridelená, preto je potrebné nastaviť rozsah nepoužitých adries. IP adresa z tohto rozsahu však bude obeti ponúknutá za predpokladu, že vyšle ako prvú správu **DHCP discover**. Pokiaľ už obeť bola pripojená v danej sieti, všesmerovo vyšle správu **DHCP request**, v ktorej žiada o IP adresu, ktorá jej už v minulosti bola pridelená. Ettercap na túto žiadosť zareaguje a vyšle obeti správu **DHCP ack**, v ktorej upraví iba parameter brány. Takto bude Ettercap reagovať aj pokiaľ sa vyčerpajú definované adresy. Parameter *Netmask* by mal obsahovať masku danej podsiete a do políčka *DNS Server IP* uvádzame IP adresu legitímnej brány. Po potvrdení tejto ponuky je útok zahájený, nástroj monitoruje sieť a čaká na DHCP správy.

Obeť sa po pripojení do prepínača prihlásila do emailovej schránky na stránke *zoznam.sk*, ktorá využíva protokol HTTP. Útočníkovi sa podarilo odchytiť ako prihlasovacie meno, tak aj heslo. Viď obr. 6.20.

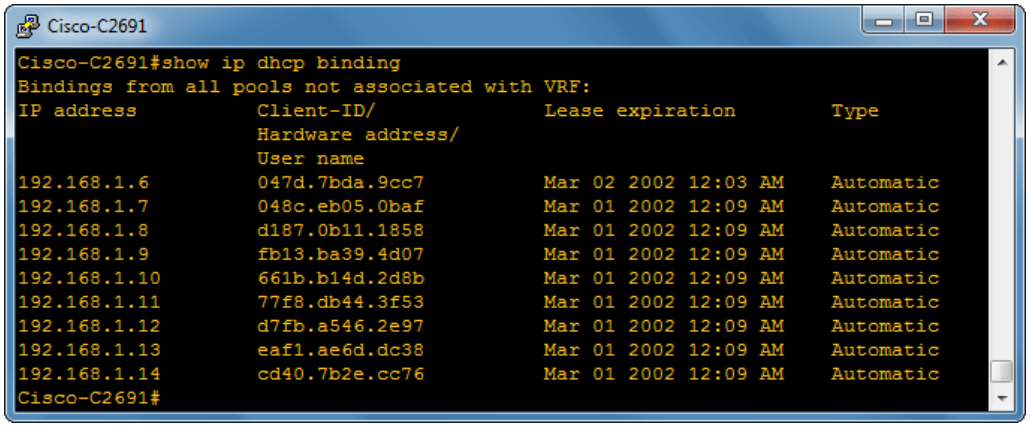
Ako je z vyššie uvedeného obrázku zrejmé, obeť po pripojení do siete vyslala správu **DHCP discover**, na ktorú Ettercap zareagoval falošnou správou **DHCP offer**, ktorou jej ponúkol podvrhnuté údaje definované podľa obr. 6.19 spolu s falošnou adresou brány. Obeť tradične pokračovala správou **DHCP request** pre ponúkanú falošnú IP adresu. Nasledovala potvrdzovacia správa **DHCP ack** od útočníka. Tým bol proces falošného prideľovania ukončený. Výpis pomocou príkazu `ipconfig` v príkazovom riadku počítača obete môžeme sledovať na obr. D.1. Avšak až po tom, ako sa celý tento proces vykonal, vyslal legitímny DHCP server správu **DHCP offer**, v ktorej klientovi ponúkal korektné údaje. To už však bolo neskoro a klient na túto správu nereagoval. Následne sa prihlásil do emailovej schránky a jeho prihlasovacie údaje boli odchytené.

Obr. 6.20: Proces útoku DHCP spoofing s odchytením prihlasovacích údajov.

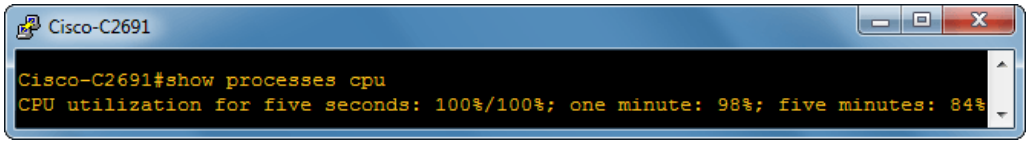
DHCP starvation

Podľa popisu v časti 3.4.1 je zrejmé, že útočníkovi ide o vyčerpanie všetkých použiteľných IP adries, ktoré ponúka DHCP server svojim klientom tým, že generuje správy **DHCP discover** s náhodnými MAC adresami.
Pri tomto útoku môžeme uvažovať topológiu na obr. 6.18 spolu s použitým prepínačom HP ProCurve 2626.
Útočník tentokrát použije nástroj Yersinia, v ktorom jednoducho bez akéhokoľvek vypĺňania údajov zahájí útok. Proces útoku môžeme pozorovať na obr. D.3. Dôsledok útoku si môžeme overiť napríklad na smerovači, na ktorom bol spustený DHCP server. Pomocou príkazu `#show ip dhcp binding` zobrazíme konkrétne adresy, ktoré boli pridelené spolu s MAC adresami. K dispozícii sú aj iné, v tomto prípade menej podstatné údaje, ako je vypršanie času prenájmu alebo typ pridelenia adresy. Ako môžeme na obr. 6.21 sledovať, celý adresný rozsah, ktorý je určený pre prideľovanie, je vyčerpaný. Tým pádom, pokiaľ sa klient pripojí do siete, neobdrží žiadne sieťové parametre a tým mu bude znemožnená komunikácia.
Okrem toho, že boli vyčerpané všetky prideliteľné IP adresy, môžeme sledovať ďalší

parazitný jav tohto útoku. Tým je nadmerné zaťaženie procesora DHCP servera, ktoré vedie k výraznému spomaleniu jeho činnosti. Tento jav môžeme skontrolovať pomocou príkazu `#show processess cpu` na konkrétnom DHCP serveri. Zaťaženie počas posledných piatich sekúnd činí 100 %, za poslednú minútu 98 % a za posledných päť minút 84 %. Viď obr. 6.22.



Obr. 6.21: Pridelené adresy DHCP serverom.



Obr. 6.22: Nadmerné zaťaženie CPU DHCP servera pri útoku DHCP starvation.

6.4.2 Aplikácia ochrany voči útoku

Najvhodnejšiu ochranu proti útoku DHCP spoofing predstavuje mechanizmus DHCP snooping. Použitý prepínač HP ProCurve túto funkciu podporuje. Pre jeho konfiguráciu boli v globálnom konfiguračnom režime na prepínač aplikované nasledovné príkazy:

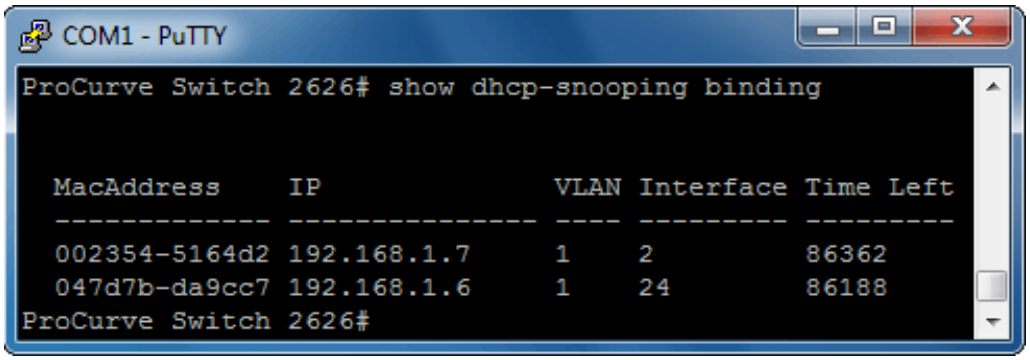
```
ProCurve_2626(config)#dhcp-snooping
ProCurve_2626(config)#dhcp-snooping authorized-server 192.168.1.5
ProCurve_2626(config)#dhcp-snooping trust eth 1
ProCurve_2626(config)#dhcp-snooping vlan 1
```

Prvým príkazom globálne aktivujeme mechanizmus DHCP snooping. V druhom príkaze pomocou parametra `authorized-server` nastavíme IP adresu legitímneho

DHCP servera. Pomocou parametra `trust` v ďalšom príkaze definujeme dôveryhodné rozhranie, čiže rozhranie, ktoré vedie k DHCP serveru. Posledným príkazom je nutné aktivovať mechanizmus pre konkrétne VLAN siete. V tomto prípade je aktivovaný pre VLAN 1, pretože podľa predvolených nastavení prepínača sú všetky rozhrania pridelené práve do VLAN 1. Viac informácií o konfigurácii mechanizmu DHCP snooping na tomto prepínači je k dispozícii na [22].
Taktiež nesmieme z hľadiska DHCP servera zabúdať na údaj *Option-82*, ktorého problém a vyriešenie bolo uvedené v časti 6.2.2. Aplikovaním týchto príkazov bol mechanizmus spustený na prepínači.

Útočník po legitímnom obdržaní IP adresy ako bežný klient zaháji útok. Po pripojení obete do prepínača Ettercap reaguje postupom, ktorý bol popísaný v časti 6.4.1. Avšak DHCP snooping na jeho činnosť reaguje a paket s ponúknutými falošnými parametrami (**DHCP offer**) ihneď zablokuje, a tak prebehne korektné pridelenie sieťových parametrov od legitímneho servera. Túto skutočnosť si môžeme overiť vypísaním štatistík procesu mechanizmu DHCP snooping pomocou príkazu `# show dhcp-snooping stats`. Viď obr. 6.23, z ktorého je možné vyčítať, že jeden paket typu *server* bol vyslaný na nedôveryhodné rozhranie a tým pádom bol zahodený. Ďalšia možnosť overenia, že mechanizmus fungoval a pridelenie parametrov bolo korektné, je vypísanie prepojení adries a ostatných údajov na prepínači, ktoré si mechanizmus svojou činnosťou vytvoril. Výpis je znázornený na obr. 6.24.

Obr. 6.23: Štatistiky procesu mechanizmu DHCP snooping.



Obr. 6.24: Korektné prepojenie adries mechanizmu DHCP snooping.

Tento mechanizmus už však nefungoval proti útoku DHCP starvation, pretože konfigurácia na danom prepínači nepodporovala nastavenie počtu prijatých DHCP správ za sekundu, poprípade tok vyjadrený v Kbit/s. Napríklad na Cisco prepínačoch je možné túto funkciu nastaviť príkazom vykonaným v konfiguračnom režime rozhrania: `#ip dhcp snooping limit rate X`, kde `X` značí počet prijatých DHCP správ za sekundu. Po prekročení tohto limitu je rozhranie deaktivované (err-disabled) a na jeho aktiváciu je potrebný zásah administrátora.
Na základe týchto faktov musela byť ako ochrana proti útoku použitá metóda zabezpečenia rozhraní. Jej aplikácia bola popísaná v časti 6.1.2. Avšak v tomto prípade je vhodnejšie znížiť limit naučených autorizovaných MAC adries na `1`, tým pádom bude povolená len MAC adresa útočníkovho PC a po zahájení útoku bude ihneď jeho rozhranie zablokované a z hľadiska DHCP servera nebude vyčerpaná žiadna prideliteľná IP adresa.

6.4.3 Vyhodnotenie útoku

Útok DHCP spoofing je útok typu MITM, no funguje len jednosmerne. Útočník teda dokáže odchytávať len trafiku smerujúcu od jeho obete do vonkajšej siete, čo predstavuje jeho nevýhodu. Avšak na odchytenie prihlasovacích údajov do služieb ako je HTTP, FTP apod. je útok dostačujúci. Ďalšiu nevýhodu predstavuje vykonateľnosť útoku len za určitých podmienok. Útok dokáže byť účinný iba v prípade, že nástroj na jeho vykonanie zachytí všesmerovú DHCP trafiku, v ktorej určité údaje podvrhne. To znamená, že po vykonaní útoku dokáže odchytávať trafiku iba od obetí, ktoré sa až následne pripojili do siete.

Útok DHCP starvation sa v prípade neprítomnosti zabezpečenia javí ako veľmi účinný DoS útok, pretože okrem znemožnenia komunikácie DHCP klientov žiadajúcich o parametre, dokáže spôsobiť aj nadmerné zaťaženie CPU DHCP servera, ktoré

vedie k výraznému spomaleniu jeho činnosti. Keďže útočník vysiela intenzívny prúd správ DHCP discover s náhodnými zdrojovými MAC adresami, môžeme taktiež pozorovať jav zaplnenia CAM tabuľky ako pri útoku MAC flooding. Ďalšou výhodou útoku je jeho jednoduchá vykonateľnosť, ktorá spočíva v niekoľkých kliknutiach GUI programu Yersinia bez nastavovania akýchkoľvek parametrov.

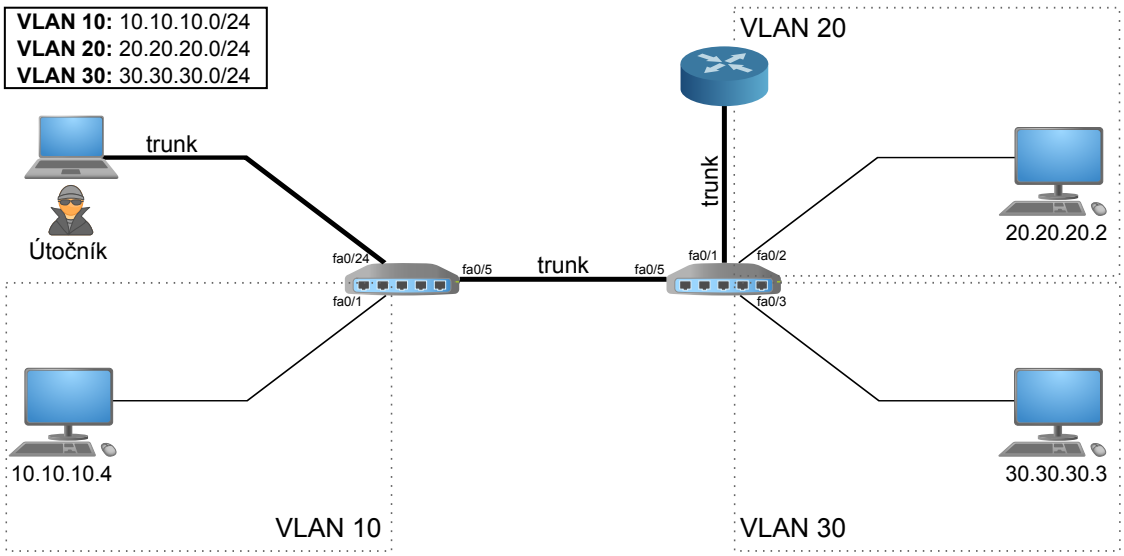
Existuje však možnosť skombinovania týchto dvoch útokov. Pokiaľ by útočník najprv vyčerpal prideliteľné adresy DHCP servera, nemusí sa nutne spoliehať, že jeho nástroj na vykonanie útoku DHCP spoofing bude rýchlejší než legitímny DHCP server. V tomto prípade bude mať istotu, že obeť obdrží ním podvrhnuté sieťové parametre. Tým sa zvýši efektivita útočnej činnosti voči protokolu DHCP.

6.5 VLAN hopping

6.5.1 Vykonanie útoku

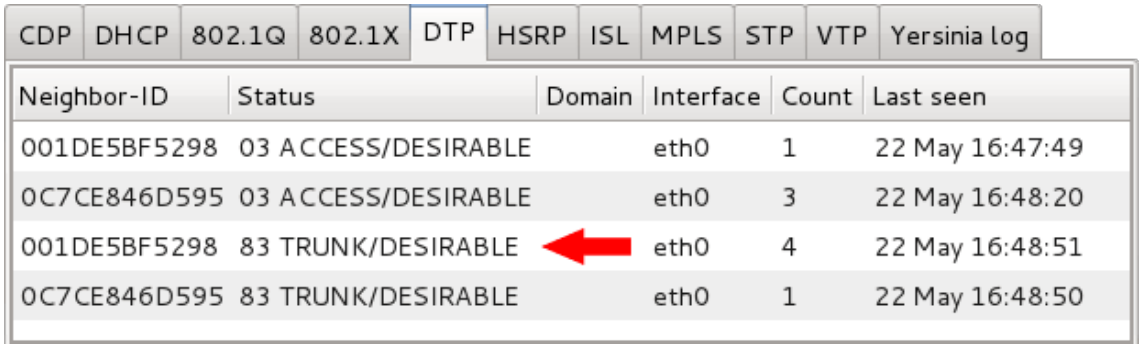
Switch spoofing

Ako bolo v časti 3.5.1 uvedené, útočníkovým cieľom je zneužitie absencie zabezpečenia protokolu DTP a následné vyjednanie trunkovej linky medzi ním a prepínačom. Tým získa prístup ku všetkým VLAN sieťam v danej manažovateľnej doméne. Použitými prepínačmi boli Cisco Catalyst 2960. Smerovač Cisco 2691 bol nasimulovaný v programe GNS3 a obsahoval konfiguráciu, ktorá umožňovala smerovanie medzi jednotlivými VLAN sieťami (Router-on-a-Stick).



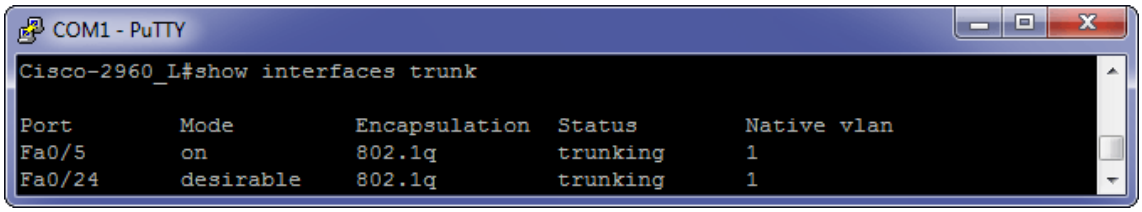
Obr. 6.25: Zapojenie zariadení pri útoku Switch spoofing.

Na vykonanie tohto útoku použil útočník grafické rozhranie nástroja Yersinia, kde v záložke „*DTP*“ zvolil možnosť „*enable trunking*“. Tým bol útok zahájený. Jeho priebeh môžeme vidieť na obr. 6.26, kde sa z prístupového režimu (*ACCESS*) zmenil útočníkovou činnosťou režim rozhrania na *TRUNK* tým, že vyslal podvrhnutý DTP paket susednému prepínaču, viď červenú šípku v obrázku.



Obr. 6.26: Vyjednanie trunkovej linky nástrojom Yersinia pri útoku Switch spoofing.

Túto skutočnosť si môžeme overiť aj na samotnom prepínači, s ktorým útočník vyjednal trunkovú linku (*fa0/24*), viď obr. 6.27.



Obr. 6.27: Zobrazenie trunkových liniek na atakovanom prepínači.

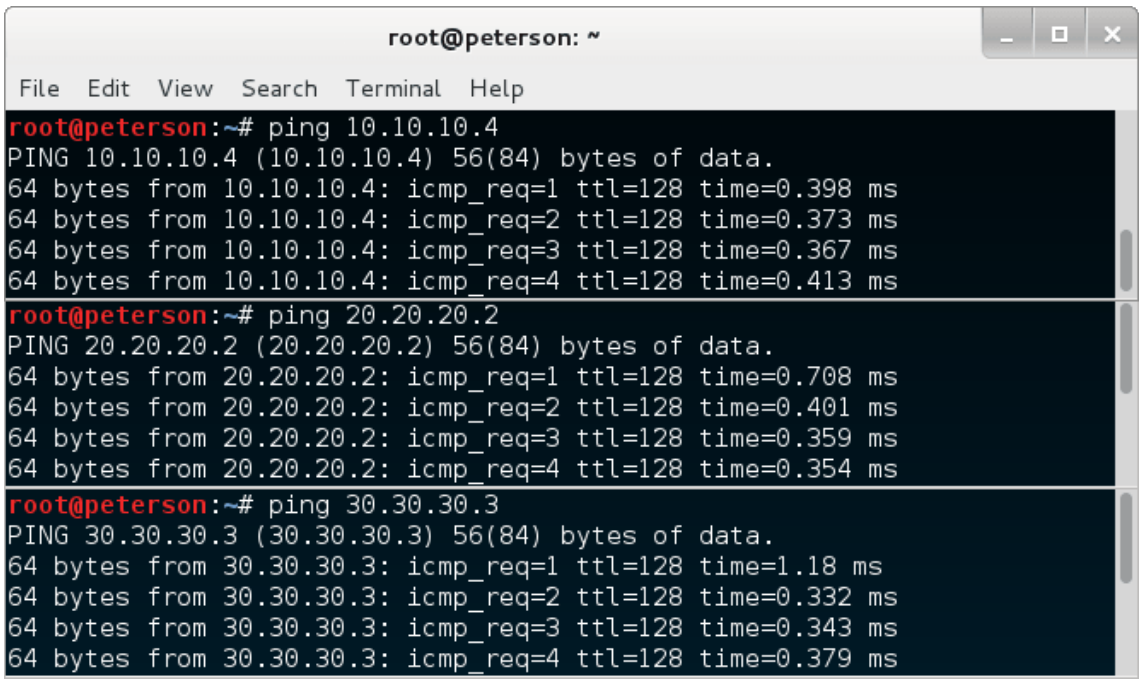
Útočník musí pre prístup do VLAN 10 dodatočne aplikovať nasledovné príkazy:

```
#modprobe 8021q
#vconfig add eth0 10
#ifconfig eth0.10 up
#ifconfig eth0.10 10.10.10.100/24
```

Prvým príkazom bol načítaný modul *802.1Q*, tým pádom aj aktivovaný tento protokol. Druhým príkazom vytvoríme takzvané podrozhranie (anglicky subinterface). Ďalším príkazom toto podrozhranie aktivujeme a posledným príkazom mu priradíme IP adresu. Ktorú IP adresu a v akom rozsahu môže útočník zistiť po vyjednaní trunkovej linky napríklad sledovaním všesmerovej trafiky na rozhraní, ktorým je do

prepínača pripojený. Obdobným spôsobom útočník nakonfiguruje aj ďalšie podrozhrania pre prístup do ostatných VLAN.

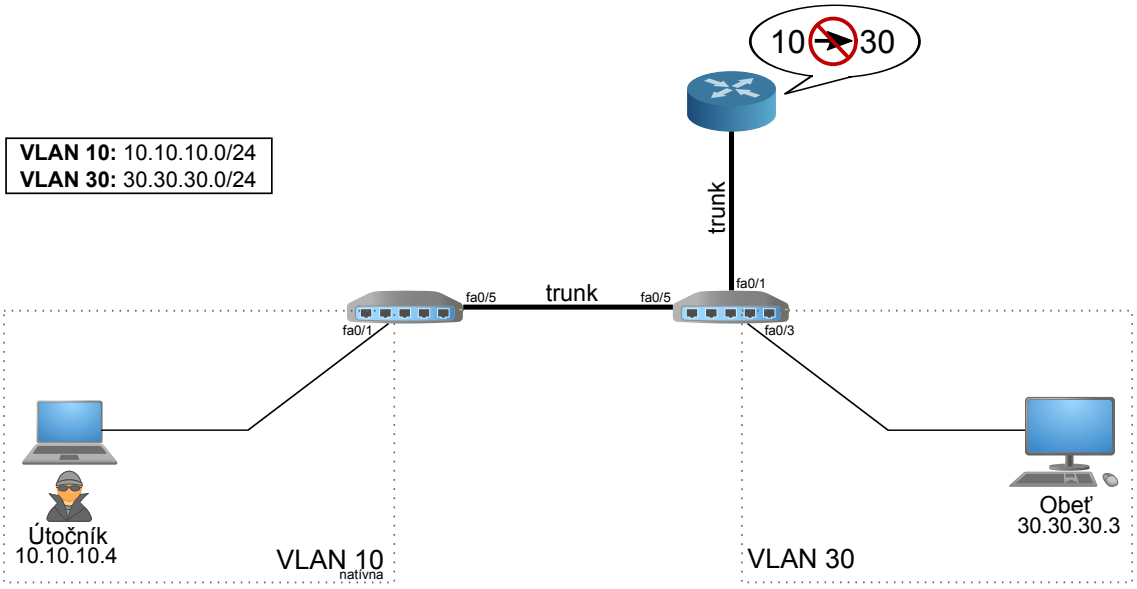
Skutočnosť, že má útočník prístup do všetkých VLAN, si môže overiť pomocou nástroja ping, viď obr. 6.28. Po tomto získaní môže útočník vykonať akýkoľvek MITM/DoS útok. Jediný rozdiel bude predstavovať fakt, že všetka trafika bude tagovaná.



Obr. 6.28: Overenie prístupu do všetkých VLAN pri útoku Switch spoofing.

Double tagging

Ako bolo uvedené v časti 3.5.1, cieľom útočníka je neautorizovaný prienik do VLAN siete, do ktorej nemá prístup. Použitými prepínačmi boli Cisco Catalyst 2950. Smerovač Cisco 2691 bol nasimulovaný v programe GNS3 a obsahoval konfiguráciu, ktorá umožňovala smerovanie medzi jednotlivými VLAN sieťami (Router-on-a-Stick), a taktiež štandardný access-list, ktorý zakazoval prístup z VLAN 10 do VLAN 30. Keďže je útok jednosmerný, jedinou možnosťou útočníka je vykonanie DoS. Na vykonanie tohto útoku je možné použiť nástroj Yersinia. Avšak tento nástroj poskytuje iba zasielanie dvojito značkovaných ICMP (ping) paketov, čo síce môže slúžiť ako demonštrácia funkčnosti útoku, no žiadnu škodlivú činnosť nespôsobí. Preto je nutné použiť tzv. packet generator.



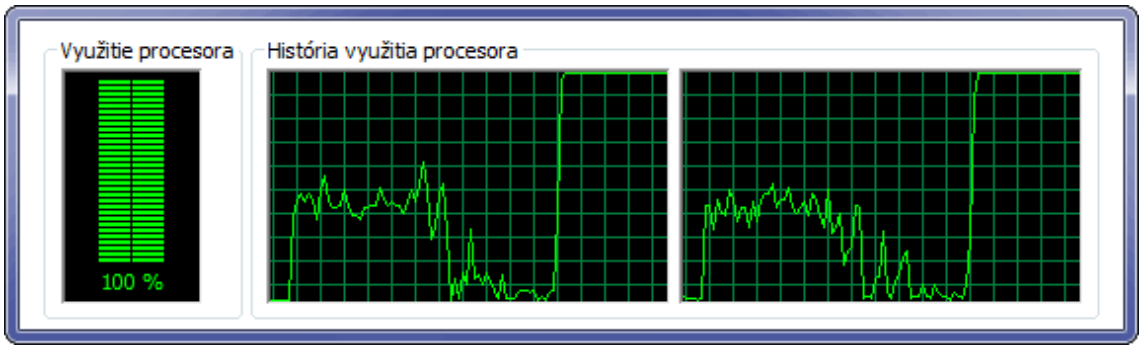
Obr. 6.29: Zapojenie zariadení pri útoku Double tagging.

Jedným z týchto generátorov je nástroj MZ (Mausezahn), ktorý však nie je súčasťou systému Kali Linux, preto je nutná jeho inštalácia. Popis tohto nástroja je dostupný na [33] a jeho manuál je možné zobraziť pomocou príkazu `#man mz`.
Útočník zadal nasledovný príkaz:

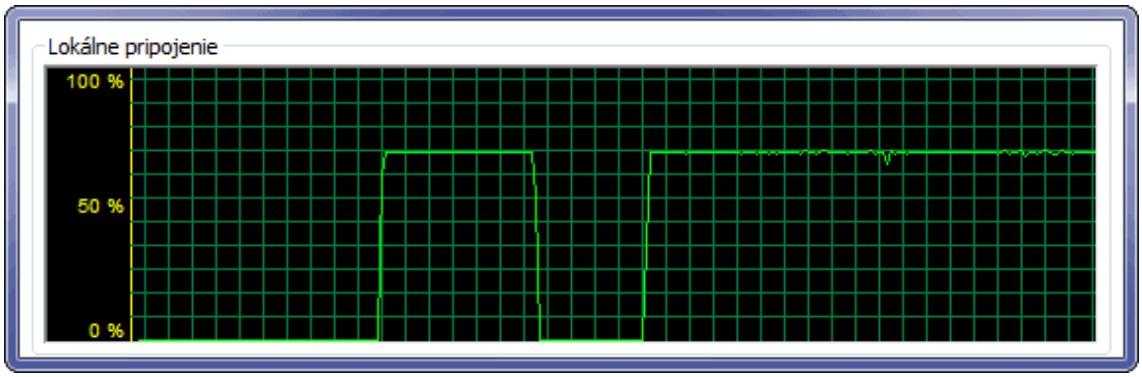
```
#mz eth0 -c 0 -Q 10,30 -A rand -B 30.30.30.0/24 -t tcp "flags=syn, dp=1-1023"
```

Parameter `-c` značí počet odoslaných paketov (hodnota *0* znamená nekonečno). Parametrom `-Q` je možné definovať dané VLAN tagy (prvý tag patrí natívnej VLAN, druhý atakovanej VLAN). Parametrom `-A` určíme zdrojovú IP adresu vyslaných paketov (*rand* značí náhodné generovanie). Parameter `-B` určuje cieľovú IP adresu (v tomto prípade bol zvolený celý adresný rozsah VLAN 30). Parameter `-t` určuje typ paketu (ďalšie možnosti sú *udp*, *arp*, *bpdu*, ...). Následne bol zvolený príznak (anglicky flag) týchto paketov a `dp` určuje cieľový port. Z vyššie uvedeného popisu môžeme určiť, že sa jedná o tzv. **TCP SYN flood** útok, ktorý bude zahlcovať adresný rozsah VLAN 30 paketmi s príznakom SYN a to na rozsah portov *1-1023*, ktoré sa nazývajú ako známe porty (anglicky well-known ports). Na týchto portoch fungujú najpoužívanejšie sieťové služby. Obvykle, podľa pravidiel o trojcestnom nadviazaní spojenia (anglicky three-way handshake), musí atakované zariadenie na správu s príznakom SYN odpovedať správou s príznakom SYN-ACK. Na tento úkon musí dané zariadenie vynaložiť určité prostriedky a cieľom útočníka je vyčerpanie týchto prostriedkov.
Potvrdením vyššie uvedeného príkazu bol útok zahájený. Súvislý tok TCP segmentov môžeme sledovať na obr. E.1 a rámec s dvomi VLAN tagmi na obr. E.2. Počítač

obete (Intel Pentium E5700 @ 3 GHz Dual Core) následne vykazoval spomalené reakcie pri každom úkone. Viď obr. 6.30, kde zaťaženie CPU atakovaného zariadenia dosahovalo hodnotu 100 %. Na obr. 6.31 môžeme sledovať zaťaženie sieťovej karty, ktoré dosahovalo hodnoty nad 70 %.



Obr. 6.30: Zaťaženie CPU atakovaného zariadenia pri útoku Double tagging.



Obr. 6.31: Zaťaženie sieťovej karty atakovaného zariadenia pri útoku Double tagging.

Väčšina prepínačov firmy Cisco využíva ako operačný systém Cisco IOS. Vyššie použité prepínače, Cisco C2950, využívajú IOS verzie 12.1. Pri použití prepínačov Cisco C2960, ktoré využívajú verzie systému IOS 12.2 a vyššie, už tento útok úspešný nebol. Jedná sa konkrétne o prepínač, do ktorého je pripojený útočník. Útok na prepínač Cisco C2960 nebol úspešný z dôvodu, že využíva práve novšiu verziu IOSu, v ktorej Cisco definovalo, že pokiaľ rozhranie v prístupovom režime príjme rámec s VLAN tagom, bude ihneď zahodený. Toto pravidlo vo verzii 12.1 definované nebolo. [34, 35]

6.5.2 Aplikácia ochrany voči útoku

Pre ochranu voči útokom spadajúcim pod VLAN hopping nie je potrebný žiadny špecializovaný mechanizmus, iba preventívne opatrenia.

Útoku Switch spoofing sa dá predísť tým, že rozhrania nenecháme v predvolenom režime (dynamic desirable), ale nastavíme ich na prístupový režim (access). V tom prípade bude útočníkovi znemožnený prvý kľúčový krok útoku – vyjednanie trunkovej linky. Rozhranie *fa0/24* uvedieme do prístupového pomocou príkazov:

```
Cisco-2950(config)# interface fa0/24
Cisco-2950(config-if)# switchport mode access
```

Ako prevencia proti útoku Double tagging sa naskytujú dve použiteľné možnosti. Prvá predstavuje uistenie sa, že natívna VLAN nie je pridelená žiadnemu prístupovému rozhraniu. Druhú možnosť, preferovanejšiu, predstavuje konfigurácia, ktorá zabezpečí, že všetka trafika, ktorá opúšťa trunk, bude tagovaná. Táto možnosť je však dostupná len na prepínačoch vyšších rádov (C3550 a vyššie). Aplikuje sa pomocou nasledovného príkazu v globálnom konfiguračnom režime:

```
Cisco-3550(config)# vlan dot1q tag native
```

Na použitý prepínač, C2950, bolo nutné použiť prvú možnosť.

6.5.3 Vyhodnotenie útoku

Útokom Switch spoofing môže útočník získať prístup ku všetkým VLAN v danej manažovateľnej doméne a následne vykonať ľubovoľný MITM/DoS útok. Avšak nevýhodu tohto útoku predstavuje práve atakovaný protokol DTP, ktorý funguje len na Cisco zariadeniach, preto nie je možné útok vykonať na zariadenia od iných výrobcov. Vďaka grafickému rozhraniu nástroja Yersinia je veľmi jednoducho vykonateľný a v prípade zanedbania vyššie uvedenej prevencie, môže predstavovať vážne bezpečnostné riziko.

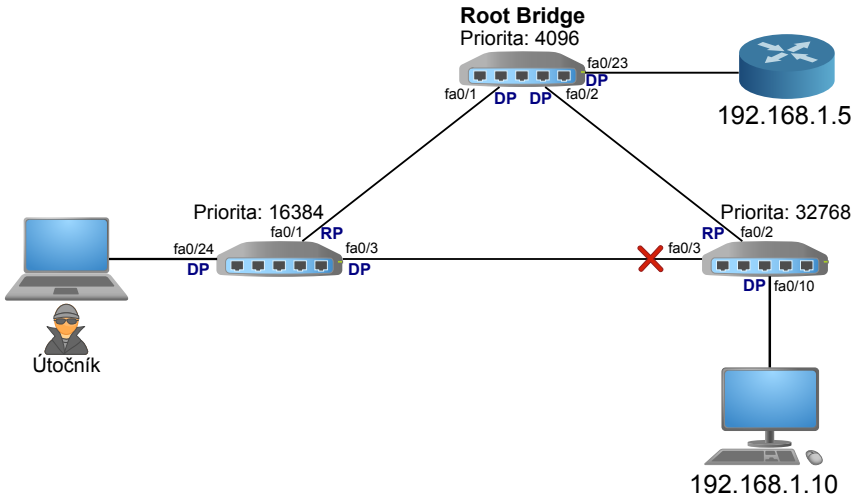
Útok Double tagging funguje len za podmienky, že útočník bude pripojený do rozhrania prepínača spadajúceho pod VLAN, ktorá je na danom trunku nastavená ako natívna, čo predstavuje značnú nevýhodu tohto útoku. Ďalšou nevýhodou tohto útoku je, že pokiaľ sa útočník pripojí do prepínača, ktorý neakceptuje tagované rámce na prístupovom rozhraní, nebude môcť útok vykonať. Avšak v prípade splnenia podmienok pre vykonanie útoku, sa za pomoci nástroja na skladanie a generovanie paketov, útok javí ako extrémne účinný DoS útok.

6.6 Útok na STP

6.6.1 Vykonanie útoku

Prevzatie role Root Bridge prepínača

Útočníkovým cieľom pri tomto útoku je zneužitie neprítomnosti autentifikačného mechanizmu protokolu STP, a tým vyjednanie role Root Bridge prepínača za účelom zmeny STP topológie. Pre bližší popis viď časť 3.6.1. Zapojenie zariadení je znázornené na obr. 6.32. Použitými prepínačmi sú Cisco C2690 ako prístupové prepínače, legitímny Root Bridge predstavuje Cisco C3550. Smerovač Cisco 2691 bol nasimulovaný v prostredí programu GNS3.



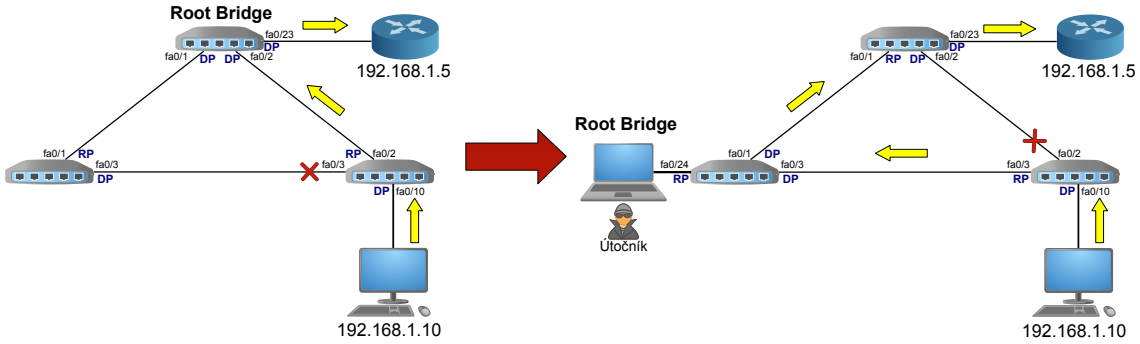
Obr. 6.32: Zapojenie pri útoku prevzatia role RB prepínača.

Útočník použil grafické rozhranie nástroja Yersinia. V záložke protokolov vybral možnosť „*STP*“ a následne zvolil „*Claiming Root Role*“. Potvrdením bol útok zahájený. Nástroj Yersinia najprv naslúcha BPDU rámce, ktoré mu prepínač pri predvolených nastaveniach posiela. V týchto rámcoch nájde informácie ako prioritu Root Bridge prepínača, jeho MAC adresu a cenu cesty, ktorú má k nemu atakovaný prepínač. To poskytne nástroju Yersinia kompletné informácie, z ktorých si môže poskladať vlastný BPDU rámec, avšak s mierne dekrementovanou hodnotou MAC adresy, čo mu zaručí nižšie BID, a tým aj rolu Root Bridge prepínača. Skutočnosť, že bola MAC adresa dekrementovaná, si môžeme overiť zachytením komunikácie v programe Wireshark, viď obr. 6.33. Okrem tohto javu môžeme z obrázku sledovať, že Root Bridge ihneď po prijatí tohto rámca odoslal správu TCN, ktorou informoval prepínače o zmene topológie. Po tejto situácii už odosielal BPDU útočník, viď zdrojovú adresu po TCN správe. Takto podvrhnuté rámce vysiela každé dve sekundy.

No.	Source	Destination	Protocol	Info
1	Cisco_6c:6f:18	Spanning-tree-STP		Conf. Root = 4096/1/00:1d:e5:bf:4f:00 Cost = 19
2	Cisco_6c:6f:18	Spanning-tree-STP		Conf. Root = 4096/1/00:1d:e5:bf:4f:00 Cost = 19
4	Cisco_6c:6f:18	Spanning-tree-STP		Conf. Root = 4096/1/00:1d:e5:bf:4f:00 Cost = 19
6	Cisco_6b:6f:00	Spanning-tree-STP		Conf. Root = 4096/1/00:1d:e5:be:4f:00 Cost = 19
7	Cisco_6c:6f:18	Spanning-tree-STP		Topology Change Notification
8	Cisco_6b:6f:00	Spanning-tree-STP		Conf. Root = 4096/1/00:1d:e5:be:4f:00 Cost = 19
9	Cisco_6b:6f:00	Spanning-tree-STP		Conf. Root = 4096/1/00:1d:e5:be:4f:00 Cost = 19
10	Cisco_6b:6f:00	Spanning-tree-STP		Conf. Root = 4096/1/00:1d:e5:be:4f:00 Cost = 19

Obr. 6.33: Zachytený proces útoku prevzatia role RB prepínača.

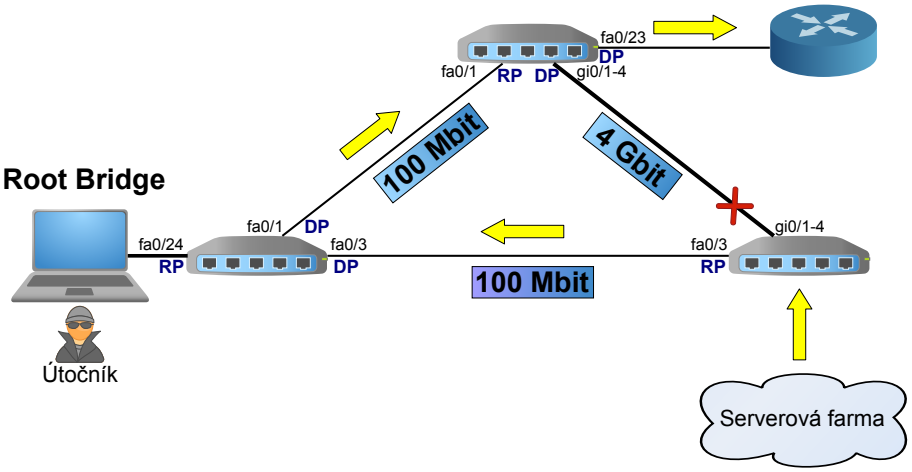
Útočník tak svojou činnosťou spôsobil zmenu STP topológie, tým pádom aj zmenu smeru dátového toku v sieti. Porovnanie je znázornené na obr. 6.34.



Obr. 6.34: Zmena STP topológie pri prevzatí role RB útočníkom.

Klient, ktorý bol pripojený do pravého prístupového prepínača, si počas útoku overoval dostupnosť smerovača nástrojom ping. Priebeh overovania môžeme sledovať na obr. F.3, z ktorého je zrejmé, že po zahájení útoku nastal približne 30 sekundový výpadok spojenia, kedy sa konvergovala zmenená STP topológia. Tento jav sa nazýva *forward delay*. Jedná sa o časový úsek, kedy predtým blokované rozhranie prechádza z takzvaného stavu *listening* (naslúchanie, 15 s), cez stav *learning* (učenie, 15 s) až do konečného stavu *forwarding* (posielanie). V stave *listening* rozhranie odosiela a prijíma BPDU správy, nie však dáta. V stave *learning* rozhranie odosiela a príjma BPDU správy, no k tomu má umožnené učenie MAC adries zariadení, ktoré si ukladá do CAM tabuľky. V stave *forwarding* je už rozhranie plne funkčné a dokáže odosielať a prijímať aj dáta. Tomuto javu je možné sa vyhnúť zavedením protokolu RSTP (Rapid STP), s ktorým konvergencia STP topológie trvá maximálne 6 sekúnd. [3]

Uvažujme však situáciu na obr. 6.35, kde namiesto klienta figuruje serverová farma, ktorá obsahuje ďalšie prepínače, do ktorých sú pripojené servery rôznych sieťových služieb, ktoré musia byť vysoko dostupné zákazníkom. Preto smerom k smerovaču vedie agregovaná linka o šírke 4 Gbit/s.



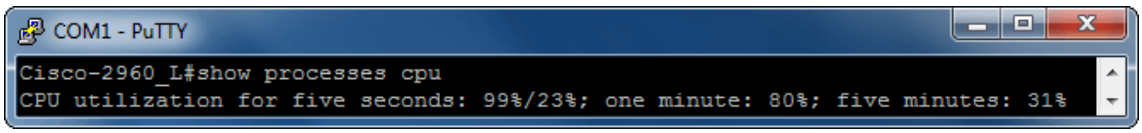
Obr. 6.35: Topológia so serverovou farmou po útoku na STP.

Pokiaľ by útočník figuroval ako Root Bridge prepínač, táto výhodná linka by bola zablokovaná, a tým by nastalo výrazné spomalenie dátového toku a zníženie dostupnosti sieťových služieb.

Zaplavenie BPDU rámcami

Útočníkovým cieľom pri tomto DoS útoku je vyčerpanie výpočtových prostriedkov atakovaného prepínača tým, že naň bude vysielať súvislý tok BPDU správ, ktoré bude prepínač musieť jednotlivo spracovať.

Útočník opäť použil nástroj Yersinia, v ktorom z ponuky zobrazenej na obr. F.1, zvolil možnosť „*sending conf BPDUs*“. Potvrdením bol útok zahájený.
Zaťaženie CPU atakovaného prepínača je zobrazené na obr. 6.36, kde úroveň zaťaženia počas posledných piatich sekúnd dosahovala 99 %. Číslo za lomítkom, čiže 23 %, značí počet percent tohto času, v ktorom bolo CPU prepínača na úrovni prerušenia. [36]



Obr. 6.36: Zaťaženie CPU prepínača pri útoku zaplavením BPDU rámcami.

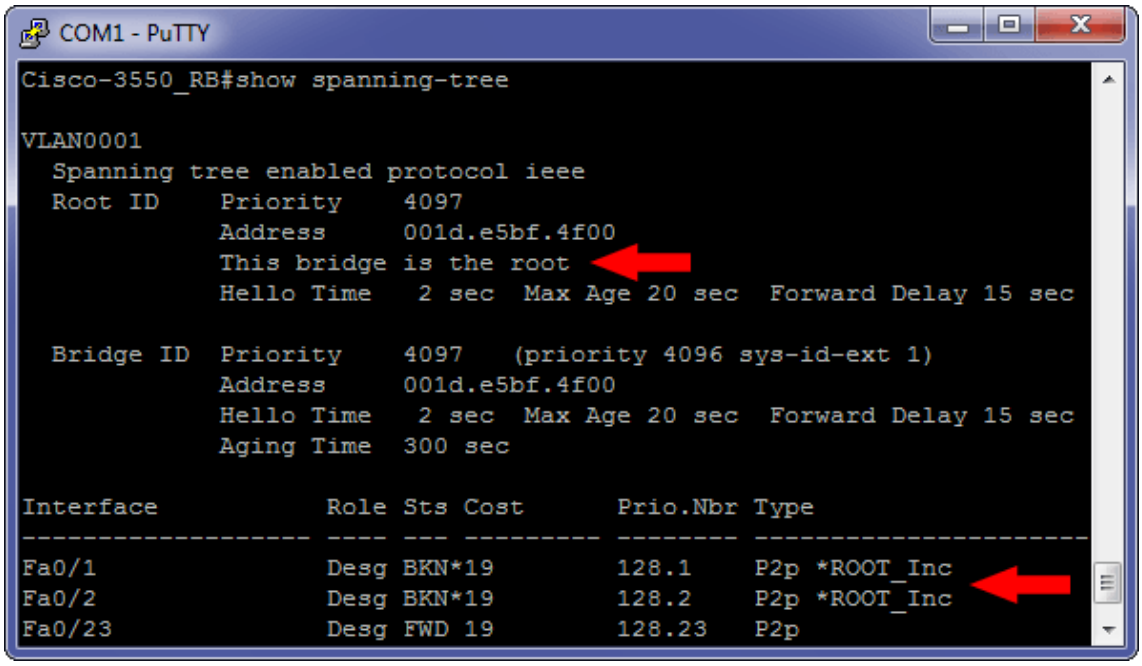
6.6.2 Aplikácia ochrany voči útoku

Root Guard

Aby sme zabránili situácii, v ktorej útočník prevezme rolu Root Bridge prepínača, máme niekoľko možností. Jednou z nich je Root Guard. Tento mechanizmus je vhodné aplikovať na rozhrania smerom k prepínačom, ktoré by sa nikdy nemali stať Root Bridge. V konkrétnej situácii (obr. 6.32) predstavuje vhodné riešenie aplikácia na rozhrania *fa0/1* a *fa0/2* Root Bridge prepínača nasledovnými príkazmi:

```
Cisco-3550_RB(config)#interface range fa0/1-2
Cisco-3550_RB(config-if)#spanning-tree guard root
```

Pokiaľ prepínač týmito rozhraniami prijíme BPDU rámec s vyšším BID ako má on sám, ihneď ich uvedie do takzvaného stavu *root-inconsistent*, až kým neprestane prijímať tieto rámce. Počas tohto stavu zahadzuje všetku sieťovú trafiku okrem legitímnych BPDU rámcov. Prepínač si tak udrží rolu Root Bridge, avšak za cenu straty konektivity pre zariadenia, ktoré chcú komunikovať s vonkajšou sieťou. Po 20 sekundách od neobdržania falošného BPDU rámca sa tento stav odstráni a rozhranie naďalej posiela a prijíma sieťovú trafiku. [3]
Vypísaním informácii o STP na danom prepínači si môžeme overiť skutočnosť, že si udržal rolu Root Bridge (prvá červená šípka), viď obr. 6.37. Taktiež môžeme vidieť stavy zablokovaných rozhraní (druhá červená šípka).



Obr. 6.37: Informácie o STP počas útoku a prítomnosti mechanizmu Root Guard.

BPDU Guard

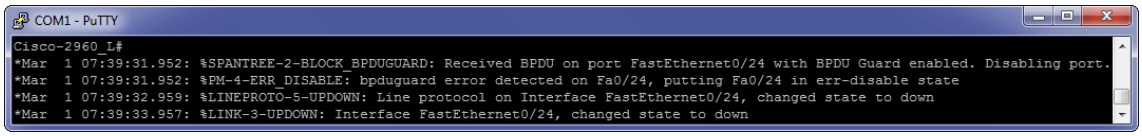
Tento mechanizmus je vhodné aplikovať na rozhrania prístupových prepínačov určené pre koncových užívateľov, ktorí žiadne BPDU produkovať nemajú, a teda by nijako nemali ovplyniť STP topológiu. Keďže BPDU Guard reaguje na akýkoľvek BPDU rámec uvedením rozhrania do *err-disabled* stavu, je tento mechanizmus vhodný aj ako ochrana proti prevzatiu role Root Bridge, aj proti zahlteniu BPDU rámcami. Konfigurácia mechanizmu môže byť vykonaná ako globálne, tak aj v režime rozhrania:

```
Cisco-2960_L(config)#spanning-tree portfast bpduguard default
```

alebo

```
Cisco-2960_L(config)#interface fa0/24
Cisco-2960_L(config-if)#spanning-tree bpduguard enable
```

Pri prvom uvedenom spôsobe sa v príkaze vyskytuje slovo *portfast*. Jedná sa o mechanizmus, ktorý umožnuje koncovým staniciam ihneď komunikovať na sieti tým, že ich rozhrania nemusia po pripojení prechádzať niekoľkými stavmi STP, a sú priamo umiestnené do stavu *forwarding*. BPDU Guard bude teda aplikovaný na všetky rozhrania, ktoré boli nakonfigurované ako *portfast*. [3]
Reakciu mechanizmu BPDU Guard na BPDU rámec môžeme vidieť na obr. 6.38.



Obr. 6.38: Reakcia mechanizmu BPDU Guard na BPDU rámec.

6.6.3 Vyhodnotenie útoku

Útočník pri prevzatí role Root Bridge prepínača spôsobí zmenu STP topológie, a tým presmerovanie sieťového toku. V prípadoch ako na obr. 6.35 môže spôsobiť výrazné spomalenie dátového toku a zníženie dostupnosti sieťových služieb. V prípade nepoužitia RSTP je ďalším parazitným javom útoku výrazný výpadok konektivity v dôsledku novej konvergencie STP topológie. Pokiaľ by útočník zahajovanie a následné ukončovanie útoku striedavo opakoval, vznikol by veľmi účinný DoS efekt.

Pokiaľ útočník zahltí atakovaný prepínač súvislým tokom BPDU správ, ktoré musia byť jednotlivo spracované, taktiež vznikne účinný DoS útok, ktorý zaťaží CPU prepínača až do oblasti maximálnych hodnôt, a tým spomalí jeho činnosť.

Oba útoky sú veľmi ľahko vykonateľné v grafickom rozhraní nástroja Yersinia.

7 CELKOVÉ VYHODNOTENIE

V minulosti sa otázka sieťových útokov týkala len vysoko znalých užívateľov, no v dnešnej dobe existujú rôzne, pre užívateľa ľahko ovládateľné nástroje s prehľadným grafickým rozhraním (Ettercap, Yersinia, ...), ktoré sú z veľkej časti automatizované. Tým pádom môže útok vykonať aj užívateľ so základnou znalosťou komunikačných mechanizmov v prepínaných LAN sieťach.

Pri realizácii vybraných útokov útočník zneužíval neprítomnosť zabezpečenia určitého protokolu, mechanizmu alebo samotného prístupu do siete. Každý útok však fungoval za určitých podmienok a zatiaľ čo v niektorých situáciach mohol fungovať podľa potreby, v iných situáciach mohol byť nepoužiteľný.

Avšak čo sa týka útokov so zámerom odchytenia citlivých údajov, najmenej kritérii na vykonanie bolo vyžadovaných pri útoku *ARP spoofing*, ktorý bol relatívne jednoducho vykonateľný, fungoval stabilne a obojsmerne, a pre bežného užívateľa nebol ľahko detegovateľný. Naopak, najmenej použiteľným útokom sa javil *MAC flooding*, ktorý pre jeho funkčné vykonanie vyžadoval veľmi špecifické podmienky.

V prípade DoS útokov bol veľmi účinným *Double tagging*, ktorý spadá pod útok *VLAN hopping*. Za pomoci generátora paketov dokázal vyťažiť aj CPU výkonnejších zariadení v celom rozsahu atakovanej VLAN. Útok však vyžadoval veľmi špecifické podmienky na vykonanie, čo predstavuje jeho výraznú nevýhodu.
Preto je možné za najúčinnejší DoS útok označiť *Útok na STP*, a to v oboch prípadoch. V prípade prevzatia role Root Bridge prepínača útočník nielenže dokázal presmerovaním trafiky výrazne spomaliť dátový tok, ale pokiaľ by zahajovanie a ukončovanie útoku striedavo opakoval, mohol by spôsobiť dlhodobý výpadok konektivity v sieti.

Detekcia a ochrana voči útokom je umožnená predovšetkým na drahších, manažovateľných prepínačoch, ktoré disponujú zobrazovacími funkciami a rôznymi ochrannými mechanizmami. Z toho vyplýva, že bežne dostupné, lacnejšie prepínače, sú vhodné predovšetkým do lokálnych sietí malých rozmerov, kde je malá pravdepodobnosť útoku a únik citlivých informácii spôsobí minimálne, respektíve zanedbateľné škody. Medzi použitými prepínačmi od firmy Cisco a HP poskytovali omnoho komplexnejšie zabezpečenie prepínače Cisco.

Za ochranu na strane aktívnych sieťových prvkov zodpovedá administrátor a uvedené ochrany, ktoré boli aplikované, je z praktického hľadiska odporúčané vhodne skombinovať. Taktiež by bolo prínosom spolu s uvedenými ochrannými opatreniami zavedenie autentifikačného protokolu, ako je *802.1X*, ktorý slúži na riadenie prístupu do siete.

Ochrana však nesmie byť opomínaná ani na strane koncového užívateľa, ktorý by mal mať aspoň základnú znalosť v oblasti bezpečnosti. Z poznatkov získaných pri vykonaných útokoch je možné odporučiť, aby mal klient nainštalovanú najnovšiu verziu webového prehliadača (iného ako Internet Explorer), viď porovnanie v tab. 6.1. Ďalej by mal použiť šifrované spojenie vždy, keď to bude možné. Mal by kontrolovať, či prihlasovací proces na ľubovoľnej stránke prebieha pomocou protokolu HTTPS a v prípade nedôveryhodnosti certifikátu danú stránku radšej opustiť. V prípade vzdialeného prístupu na zariadenia výlučne nepoužívať protokol Telnet, ale SSH, a to jedine vo verzii 2. V nastaveniach SSH klientov je možné zvoliť výhradné použitie tejto verzie, ktorá už poskytuje omnoho bezpečnejší ochranný mechanizmus na rozdiel od verzie 1. Taktiež pri prenose súborov by mal užívateľ uprednostniť zabezpečené protokoly ako SFTP alebo FTPS.

Po dodržaní vyššie uvedených bezpečnostných opatrení, či už na strane administrátora, alebo koncového užívateľa, bude mať útočník výrazne sťaženú situáciu pri vykonávaní škodlivej činnosti v prepínanej LAN sieti.

8 ZÁVER

Cieľom bakalárskej práce bolo zmapovať najčastejšie útoky na prepínače, vybrané útoky prakticky uskutočniť a na základe týchto poznatkov vykonať ich zhodnotenie.

Teoretická časť práce sa delí do piatich hlavných častí. Prvá časť mapuje technológie Ethernet a ich základné pojmy, druhá časť patrí prepínaču a jeho základnej charakteristike a funkciám. Tretia, najobsiahlejšia teoretická časť, je venovaná samotným útokom na prepínače. Ku každému útoku bol uvedený jeho teoretický popis, možná detekcia a ochrana voči nemu. Ďalšia teoretická časť popisuje programové vybavenie, ktoré bolo použité na vykonanie vybraných útokov. Posledná, piata teoretická časť, sa venuje popisu použitých prepínačov. Konkrétne sa jedná o prepínače od firmy Hewlett-Packard a Cisco, ktoré patria medzi najpoužívanejšie v inštitučnom prostredí.

Praktická časť práce je venovaná vykonaniu vybraných útokov, ktoré boli v teoretickej časti popísané. Pri každom jednotlivom útoku je uvedený postup na jeho vykonanie, aplikácia ochrany voči nemu a jeho vyhodnotenie.
Práca sa zaoberala šiestimi útokmi. Jedná sa o *MAC flooding*, *ARP spoofing*, *Port stealing*, *Útok na DHCP*, *VLAN hopping* a *Útok na STP*. Všetky útoky boli vykonávané v laboratórnych podmienkach a zapojenia jednotlivých zariadení sa podľa možností snažili o čo najautentickejšie principiálne napodobenie praktickej situácie, ktorá môže v inštitučnom prostredí nastať. Ku každému útoku sú ďalej v prílohách uvedené dodatočné snímky, ktoré slúžia k bližšiemu popisu priebehu alebo dopadu jednotlivých útokov.

Na základe poznatkov z teoretickej a praktickej časti bolo vykonané celkové vyhodnotenie práce, v ktorom sú určité útoky porovnané z hľadiska ich vykonateľnosti a účinnosti. Ďalej je tu uvedený odporúčaný spôsob zabezpečenia a prevencie ako zo strany administrátora, tak aj zo strany koncového užívateľa.

LITERATÚRA

[1] DOSTÁLEK, L. *Velký průvodce protokoly TCP/IP: Bezpečnost*. 1. vyd. Praha: Computer Press, 2001. 565 s. ISBN 80-722-6513-X.

[2] VYNCKE, E.; PAGGEN C. *LAN Switch Security: What Hackers Know About Your Switches*. 1. vyd. Indianapolis: Cisco Press, 2008. 360 s. ISBN 978-1-58705-256-9.

[3] HUCABY, D. *CCNP SWITCH 642-813 Official Certification Guide*. 1. vyd. Indianapolis: Cisco Press, 2010. 459 s. ISBN 978-1-58720-243-8.

[4] HUCABY, D. *CCNP BCMSN Exam Certification Guide, 3rd Edition*. 3. vyd. Indianapolis: Cisco Press, 2005. 624 s. ISBN 978-1-58720-142-4.

[5] SEIFERT, R.; EDWARDS, J. *The Complete Guide to LAN Switching Technology, Second Edition*. 2. vyd. Indianapolis: Wiley, 2008. 818 s. ISBN 978-0-470-28715-6.

[6] LAMMLE, T. *CCNA: Cisco Certified Network Associate Fast Pass – 3rd ed.* 3. vyd. Indianapolis: Wiley, 2007. 504 s. ISBN 978-0-470-18571-1.

[7] CASTELI, M. *LAN Switching First-Step*. 1. vyd. Indianapolis: Cisco Press, 2005. 408 s. ISBN 978-1-58720-100-4.

[8] KENNEDY, C.; HAMILTON, K. *Cisco LAN Switching*. 1. vyd. Indianapolis: Cisco Press, 1999. 960 s. ISBN 1-57870-094-9.

[9] LEE, M. *Address Resolution Protocol Risks and Countermeasures* [online]. 19. 12. 2004, [cit. 6. 12. 2013]. 58 s. Dostupné z WWW: <`http://it-audit.sans.org/community/papers/address-resolution-protocol-risks-countermeasures_186`>.

[10] SPANGLER, R. *Packet Sniffing on Layer 2 Switched Local Area Networks* [online]. 2013, [cit. 8. 12. 2013]. 7 s. Dostupné z WWW: <`http://www.rootsecure.net/content/downloads/pdf/layer2sniffing.pdf`>.

[11] ZUZČÁK, M. *Bezpečnosť na LAN pod lupou: Úvod a útok ARP cache poisoning* [online]. 5. 7. 2011, [cit. 14. 12. 2013]. Dostupné z WWW: <http://www.secit.sk/sk/content/bezpecnost-na-lan-pod-lupou-uvod-utok-arp-cache-poisoning>.

[12] ZUZČÁK, M. *Bezpečnosť na LAN pod lupou: Port stealing a MAC flooding* [online]. 19. 7. 2011, [cit. 14. 12. 2013]. Dostupné z WWW: <http://www.secit.sk/sk/content/bezpecnost-na-lan-pod-lupou-port-stealing-mac-flooding>.

[13] LIČMAN, P., et al. *Možnosti DHCP snoopingu, relayingu a podpora multicastingu na DSLAM Zyxel IES-1000* [online]. 2008, [cit. 15. 12. 2013]. 18 s. Dostupné z WWW: <http://wh.cs.vsb.cz/sps/images/0/01/DSLAM_DHCPaMulticast.pdf>.

[14] ODOM, W. *CCENT/CCNA ICND1 640-822 Official Cert Guide, Third Edition.* 3. vyd. Indianapolis: Cisco Press, 2012. 1015 s. ISBN 978-1-58720-425-8.

[15] ZUZČÁK, M. *Bezpečnosť na LAN pod lupou: DHCP spoofing* [online]. 11. 8. 2011, [cit. 16. 12. 2013]. Dostupné z WWW: <http://www.secit.sk/sk/content/bezpecnost-na-lan-pod-lupou-dhcp-spoofing>.

[16] KOZIEROK, C. *DHCP Parameter Configuration Process For Clients With Non-DHCP Addresses* [online]. 20. 9. 2005, [cit. 16. 12. 2013]. Dostupné z WWW: <http://www.tcpipguide.com/free/t_DHCPParameterConfigurationProcessForClientsWithNon-2.htm>.

[17] BALCHUNAS, A. *CCNA Study Guide v2.62* [online]. 2012, [cit. 16. 12. 2013]. 304 s. Dostupné z WWW: <http://www.routeralley.com/ra/completed/ccna_studyguide.pdf>.

[18] *What is Kali Linux?* [online]. [cit. 1. 4. 2014]. Dostupné z WWW: <http://docs.kali.org/introduction/what-is-kali-linux>.

[19] *Flood network with random MAC addresses with macof tool* [online]. 4. 3. 2011, [cit. 31. 12. 2013]. Dostupné z WWW: <http://tournasdimitrios1.wordpress.com/2011/03/04/flood-network-with-random-mac-addresses-with-macof-tool>.

[20] *Sniffing hesiel v Ettercap-ng.* In: *Serverfault* [online]. 22. 5. 2010, [cit. 31. 12. 2013]. Dostupné z WWW: <http://www.serverfault.sk/2010/05/sniffing-hesiel-v-ettercap-ng>.

[21] YERSINIA, Oficiálne stránky produktu [online]. [cit. 1. 1. 2014]. Dostupné z WWW: <http://www.yersinia.net>.

[22] HP PROCURVE SERIES 2600, softvérová dokumentácia [online]. [cit. 10. 4. 2014]. Dostupné z WWW: <http://cdn.procurve.com/training/Manuals/2600-RelNotes-H1083-59906003.pdf>.

[23] CISCO CATALYST 2950, dokumentácia zariadenia [online]. [cit. 10. 4. 2014]. Dostupné z WWW: <http://www.andovercg.com/datasheets/cisco-2950-standard-image.pdf>.

[24] CISCO CATALYST 2960, dokumentácia zariadenia [online]. [cit. 10. 4. 2014]. Dostupné z WWW: <http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-series-switches/product_data_sheet0900aecd80322c0c.html>.

[25] CISCO CATALYST 3550, dokumentácia zariadenia [online]. [cit. 10. 4. 2014]. Dostupné z WWW: <http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3550-series-switches/product_data_sheet09186a00800913d7.html>.

[26] *Configuring and Monitoring Port Security* [online]. [cit. 10. 5. 2014]. Dostupné z WWW: <ftp://ftp.hp.com/pub/networking/software/Security-Oct2005-59906024-Chap09-Port_Security.pdf>.

[27] PURSER, J. *SSHv1 or SSHv2? What's the big deal?* [online]. 22. 9. 2008, [cit. 18. 5. 2014]. Dostupné z WWW: <https://learningnetwork.cisco.com/blogs/network-sheriff/2008/09/22/sshv1-or-sshv2-whats-the-big-deal>.

[28] *ETTERCAP - The Easy Tutorial - Man in the middle attacks* [online]. 10. 3. 2008, [cit. 18. 5. 2014]. Dostupné z WWW: <http://openmaniak.com/ettercap_filter.php>.

[29] *Configuring DHCP Features* [online]. [cit. 19. 5. 2014]. Dostupné z WWW: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-1_19_ea1/configuration/guide/3550scg/swdhcp82.html>.

[30] *Configuring the DHCP Option 82 for Subscriber Identification* [online]. [cit. 19. 5. 2014]. Dostupné z WWW: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-1_13_ea1/configuration/guide/3550scg/swdhcp82.html>.

[31] *Configuring Dynamic ARP Inspection* [online]. [cit. 19. 5. 2014]. Dostupné z WWW: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-2_25_see/configuration/guide/3550SCG/swdynarp.html>.

[32] *Catalyst 2960 and 2960-S Switch Cisco IOS Commands - shutdown through vtp* [online]. [cit. 22. 5. 2014]. Dostupné z WWW: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_53_se/command/reference/2960ComRef/cli3.html#wp1948361>.

[33] MAUSEZAHN, Oficiálne stránky produktu [online]. [cit. 24. 5. 2014]. Dostupné z WWW: <http://www.perihel.at/sec/mz/>.

[34] *Configuring Interface Characteristics (C2950)* [online]. [cit. 24. 5. 2014]. Dostupné z WWW: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2950/software/release/12-1_19_ea1/configuration/guide/2950scg/swint.html>.

[35] *Configuring Interface Characteristics (C2960)* [online]. [cit. 24. 5. 2014]. Dostupné z WWW: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swint.html>.

[36] *The show processes Command* [online]. [cit. 25. 5. 2014]. Dostupné z WWW: <http://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-120-mainline/15102-showproc-cpu.html>.

[37] *highspeedbackbone.net* [online]. [cit. 10. 4. 2014]. Dostupné z WWW: <http://images.highspeedbackbone.net/skuimages/large/H24-J4900A.jpg>.

[38] *devicespec.net* [online]. [cit. 10. 4. 2014]. Dostupné z WWW: <http://devicespec.net/images/ws-c2950c-24_image001.jpg>.

[39] *ciscocentral.com.au* [online]. [cit. 11. 4. 2014]. Dostupné z WWW: <http://www.ciscocentral.com.au/Images/Product/WS-C2960-x%2024.jpg>.

[40] *cablesandkits.com* [online]. [cit. 11. 4. 2014]. Dostupné z WWW: <http://media.cablesandkits.com/ipn/WSC355024PWRSMIa.jpg>.

ZOZNAM SKRATIEK

ARP Address Resolution Protocol

BPDU Bridge Protocol Data Unit

CAM Content Addressable Memory

CDP Cisco Discovery Protocol

CPU Central Processing Unit

CRC Cyclic Redundancy Check

CSMA/CD Carrier Sense Multiple Access with Collision Detection

DAI Dynamic Address Resolution Protocol Inspection

DAP Dynamic Address Resolution Protocol Protection

DHCP Dynamic Host Configuration Protocol

DNS Domain Name System

DoS Denial of Service

DTP Dynamic Trunking Protocol

FCS Frame Check Sequence

FDDI Fiber Distributed Data Interface

FTP File Transfer Protocol

FTPS FTP over SSL

gARP gratuitous Address Resolution Protocol

HSRP Hot Standby Router Protocol

HTML HyperText Markup Language

ICMP Internet Control Message Protocol

IEEE Institute of Electrical and Electronics Engineers

IOS Internetwork Operating System

IP Internet Protocol

ISL Inter-Switch Link Protocol

ISO International Organization for Standardization

LAN Local Area Network

MAC Media Access Control

MITM Man-In-The-Middle

NAT Network Address Translation

OSI Open Systems Interconnection

OUI Organizationally Unique Identifier

PDU Protocol Data Unit

QoS Quality of Service

RAM Random Access Memory

RSTP Rapid Spanning Tree Protocol

SFD Start Frame Delimiter

SFTP SSH File Transfer Protocol

SNMP Simple Network Management Protocol

SSH Secure Shell

SSL Secure Sockets Layer

STP Spanning Tree Protocol

TCN Topology Change Notification

TCP Transmission Control Protocol

TTL Time to Live

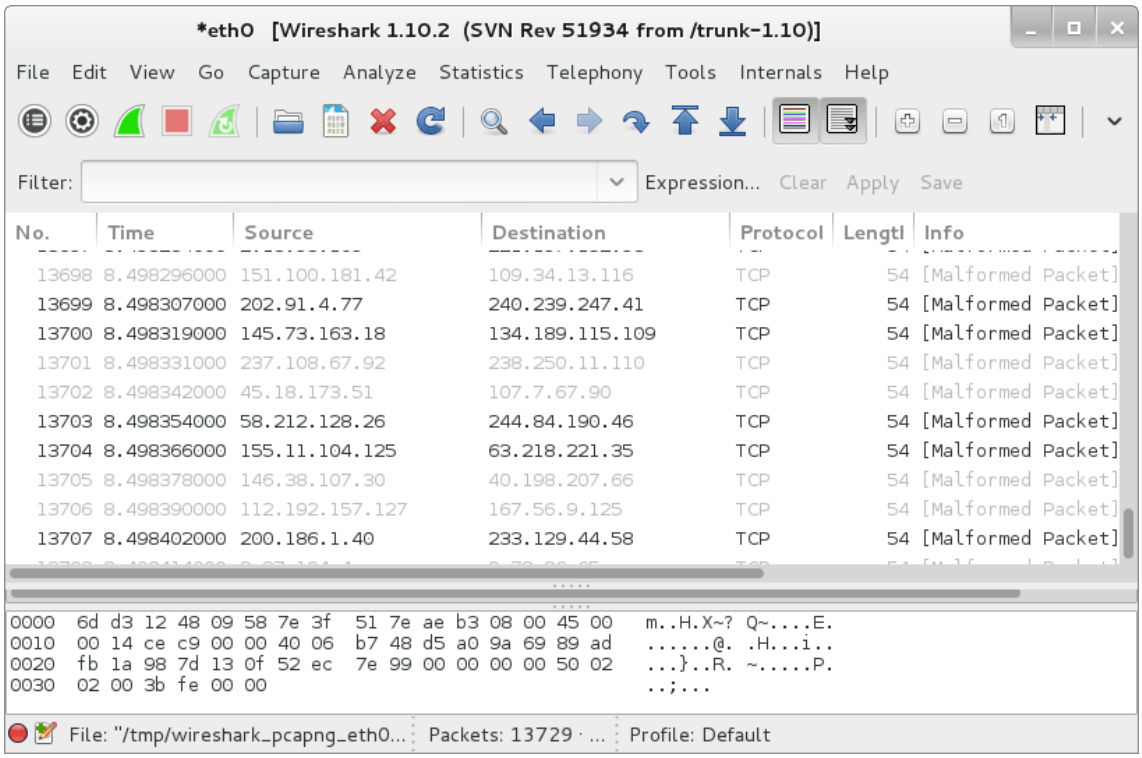
VLAN Virtual Local Area Network

VTP VLAN Trunking Protocol

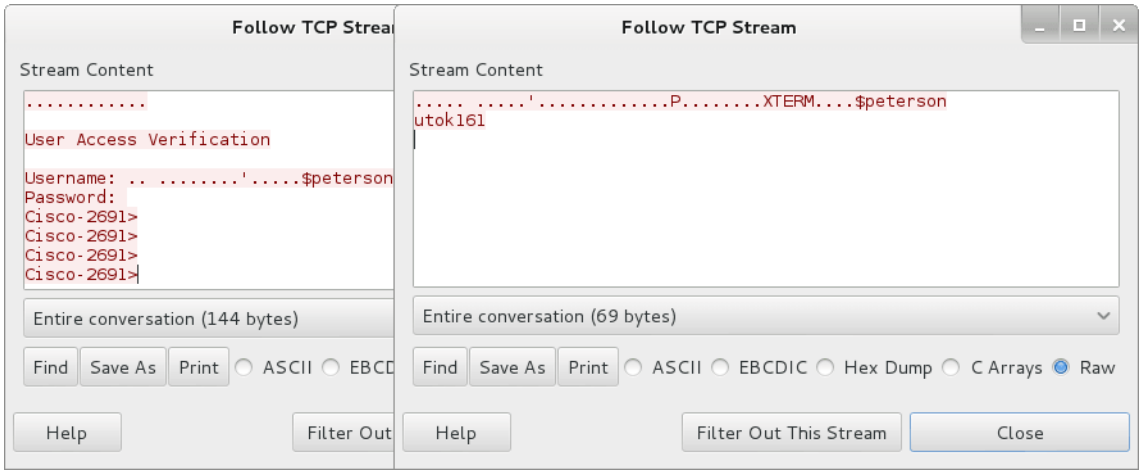
WAN Wide Area Network

ZOZNAM PRÍLOH

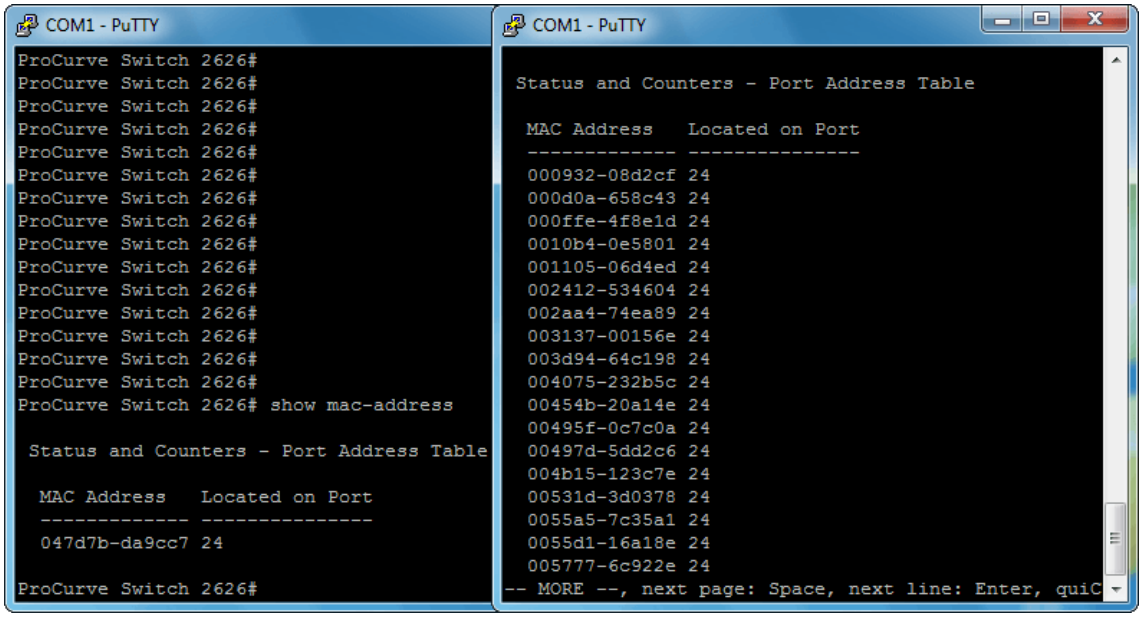
A PRÍLOHA K ÚTOKU MAC FLOODING



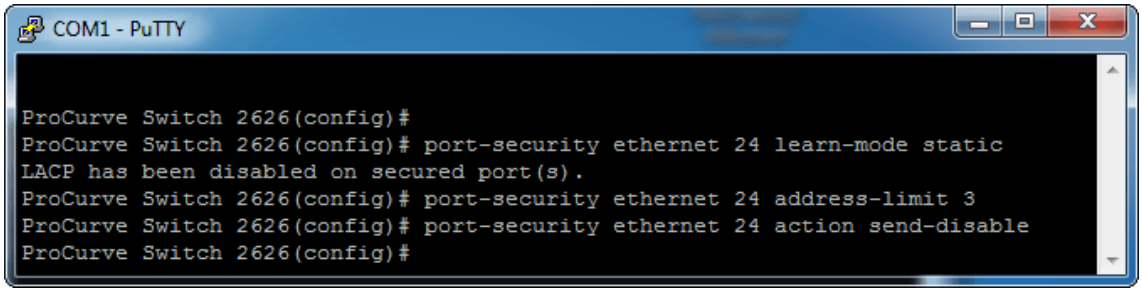
Obr. A.1: Prúd rámcov vygenerovaný nástrojom Macof.



Obr. A.2: Neúplné odchytenie komunikácie služby telnet.

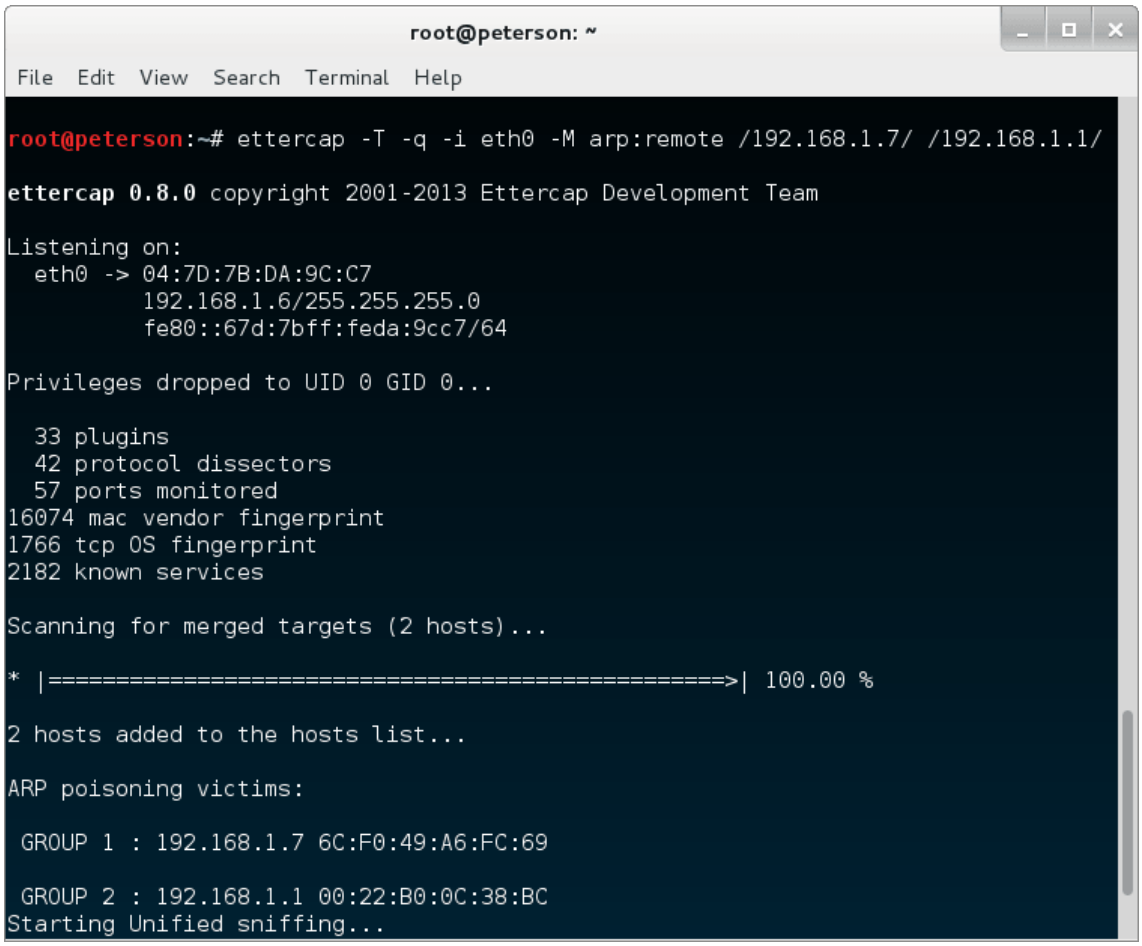


Obr. A.3: Porovnanie CAM tabuľky prepínača pred a po útoku.

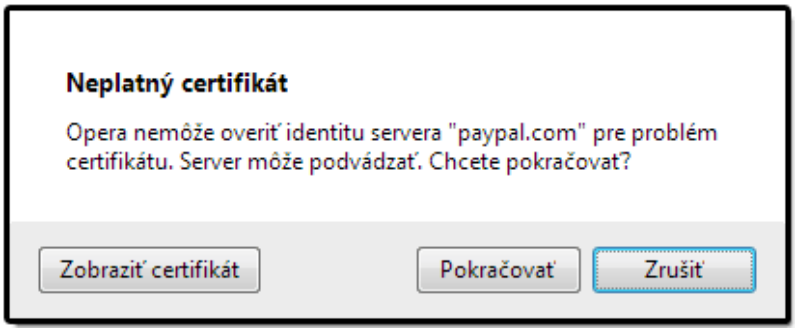


Obr. A.4: Zabezpečenie rozhrania na HP ProCurve 2626.

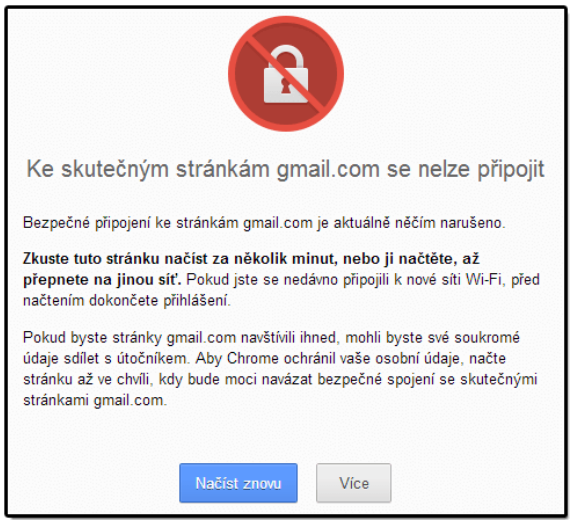
B PRÍLOHA K ÚTOKU ARP SPOOFING



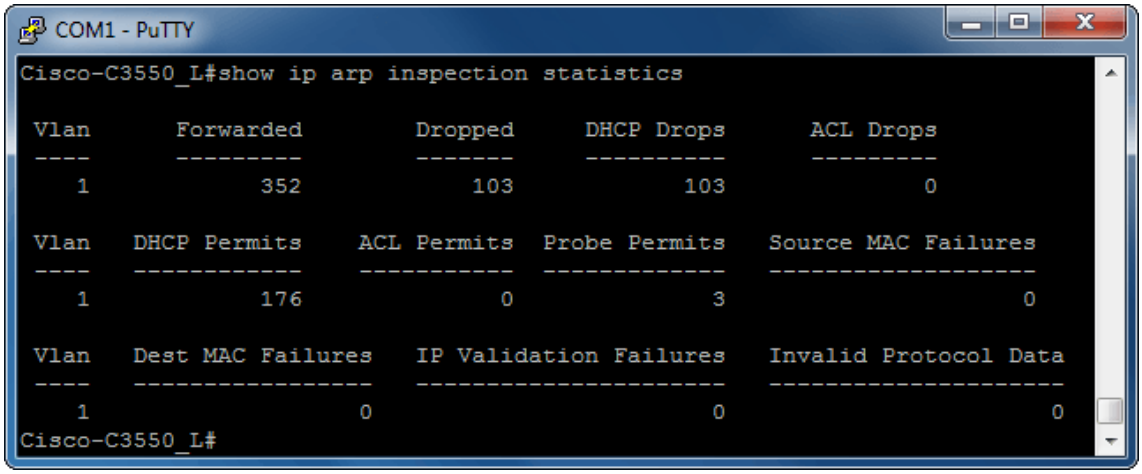
Obr. B.1: Zahájenie útoku ARP spoofing.



Obr. B.2: Upozornenie na bezpečnostné riziko prehliadačom Opera.

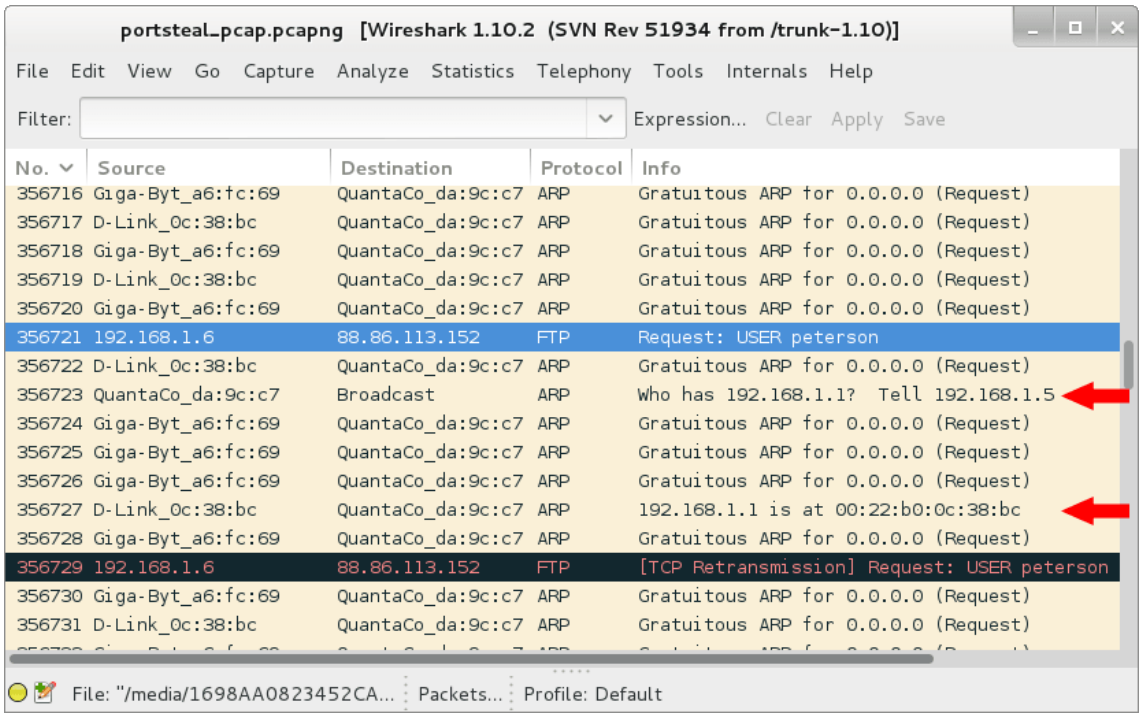


Obr. B.3: Zablokovanie prístupu na stránku prehliadačom Google Chrome.



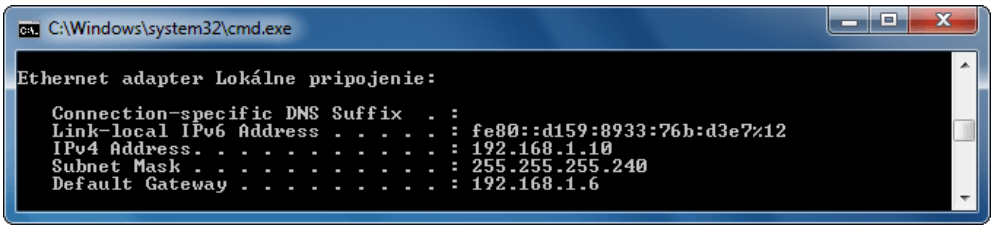
Obr. B.4: DAI štatistika preposlaných a zahodených ARP paketov.

C PRÍLOHA K ÚTOKU PORT STEALING

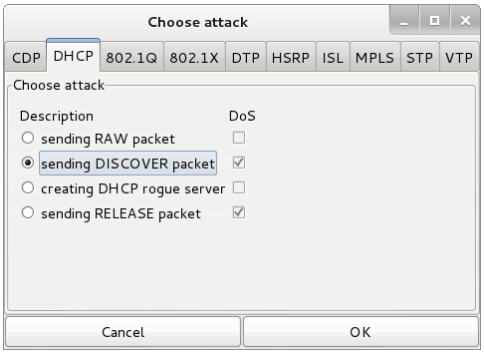


Obr. C.1: Zachytený priebeh útoku Port stealing.

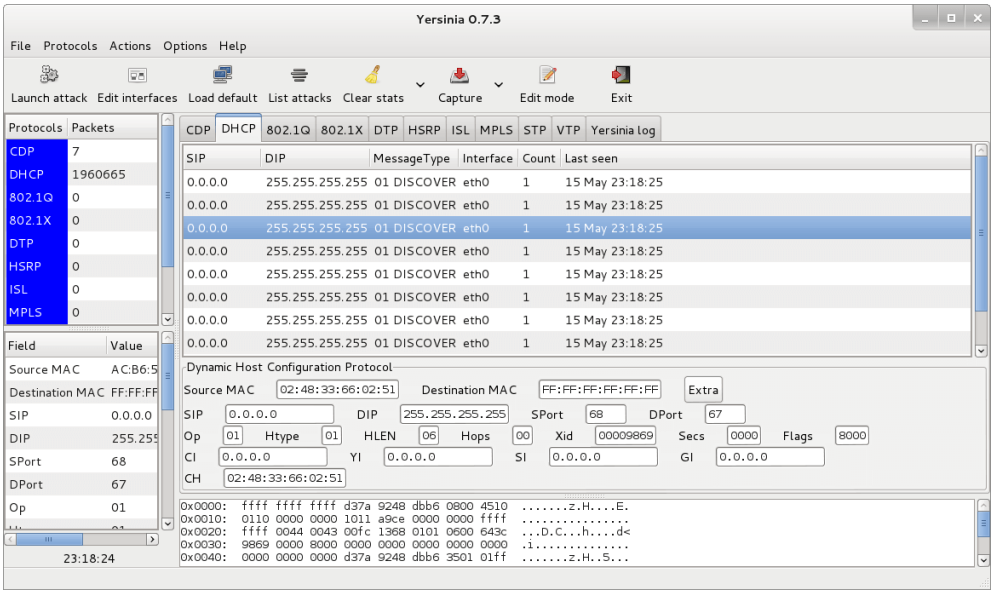
D PRÍLOHA K ÚTOKU NA DHCP



Obr. D.1: Podvrhnuté sieťové parametre na počítači obeti.

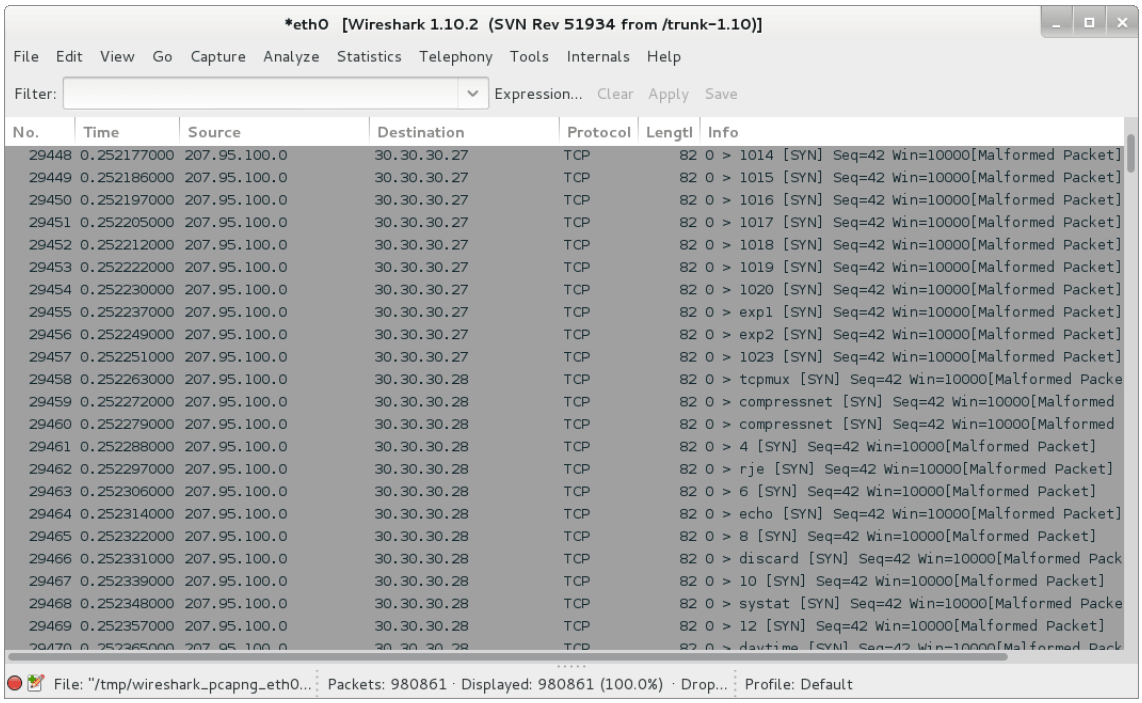


Obr. D.2: Zahájenie útoku DHCP starvation.

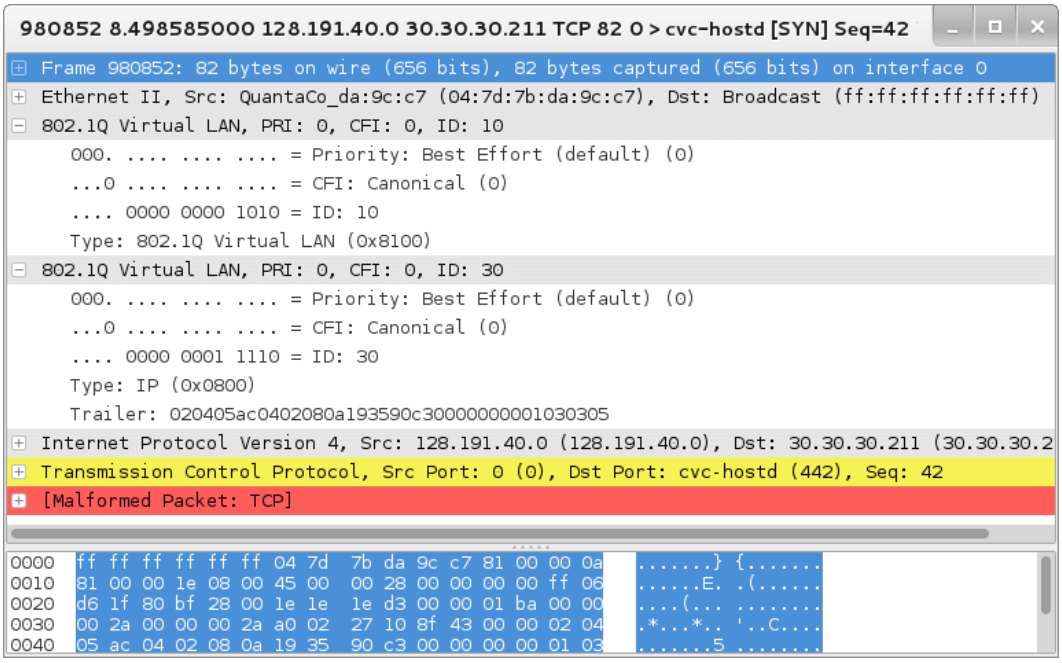


Obr. D.3: Proces útoku DHCP starvation.

E PRÍLOHA K ÚTOKU VLAN HOPPING

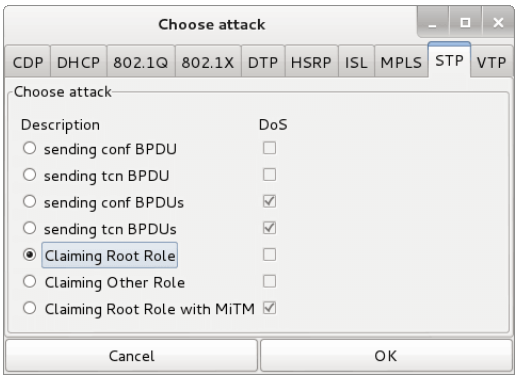


Obr. E.1: Tok TCP segmentov pri útoku Double tagging.



Obr. E.2: Odchytený rámec s dvomi VLAN tagmi počas útoku Double tagging.

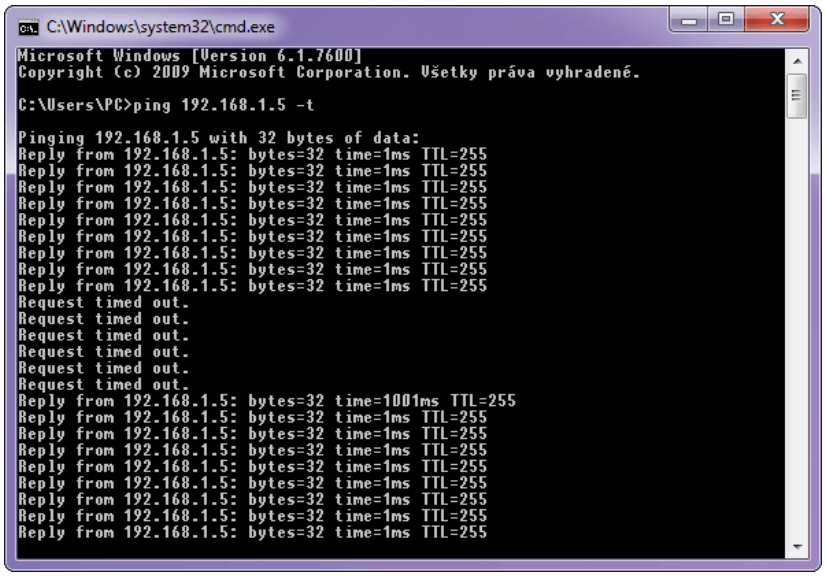
F PRÍLOHA K ÚTOKU NA STP



Obr. F.1: Zahájenie útoku prebratia Root Bridge prepínača.

```
Cisco-2960_L#
STP: VLAN0001 heard root  4097-001d.e5be.4f00 on Fa0/24
    supersedes  4097-001d.e5bf.4f00
STP: VLAN0001 new root is 4097, 001d.e5be.4f00 on port Fa0/24, cost 38
STP: VLAN0001 Topology Change rcvd on Fa0/1
STP: VLAN0001 sent Topology Change Notice on Fa0/24
STP: VLAN0001 Topology Change rcvd on Fa0/3
```

Obr. F.2: Zaznamenanie zmeny Root Bridge ľavým prístupovým prepínačom.



Obr. F.3: Overovanie dostupnosti smerovača počas útoku na STP.

G OBSAH PRILOŽENÉHO CD

Priložené CD obsahuje elektronickú verziu práce vo formáte PDF.